Aareal
YOUR COMPETITIVE ADVANTAGE.

Aareal Portal

Handbuch für Administratoren

Impressum

Dokumentation des Aareal Portals, Release 7.8.4 vom 17.01.2023

Aareal Bank AG
Geschäftsbereich Banking & Digital Solutions
Paulinenstraße 15
65189 Wiesbaden

Inhalt

1. Einführung 5
2. Voraussetzungen 7
3. Schnelleinstieg: Wie kann ich …? 8
4. In wenigen Schritten zum einsatzbereiten Aareal Portal 11
5. Benutzer einrichten 13
   5.1. Einen neuen Benutzer anlegen oder einen bestehenden Benutzer ändern 18
   5.2. Benutzer sperren 23
   5.3. Einen weiteren Administrator anlegen lassen 24
   5.4. Einem Benutzer neue Zugangsdaten vergeben 25
   5.5. Ein Schlüsselmedium durch den Administrator freischalten 25
   5.6. Ihr eigenes Passwort ändern 26
6. Rollen und Rechte 28
   6.1. Rollen anlegen und verwalten 28
   6.2. Kontoeinschränkungen anlegen und verwalten 31
7. Verwaltung der imageTAN-Reader 35
   7.1. Aktivierte imageTAN-Lizenzen einsehen und freigeben 35
   7.2. Einstellungen am imageTAN-Reader vornehmen 36
   7.3. Fehlerzustände beheben 37
      7.3.1. Der Benutzer hat seine PIN vergessen 37
      7.3.2. Der Benutzer hat sein Gerät durch Falscheingabe der PIN gesperrt 37
      7.3.3. Der Benutzer hat seinen imageTAN-Reader verloren 39
      7.3.4. Ein verlorener imageTAN-Reader taucht wieder auf 40
8. Benutzern EBICS-Teilnehmer zuordnen 42
9. Abrufmanager 45
10. Aktivitätenprotokolle 46
11. Abbildungsverzeichnis 48
12. Tabellenverzeichnis 49

1. Einführung

Herzlich willkommen zum Handbuch für Administratoren im Aareal Portal!

Das Aareal Portal unterstützt Sie und Ihre Mitarbeiter in Ihren finanziellen Belangen, unabhängig davon, ob Sie in einem dynamischen, kleinen Unternehmen mit wenigen Mitarbeitern arbeiten, oder ob Sie mit einer größeren Zahl an Mitarbeitern komplexe Arbeitsabläufe zur Freigabe und Prüfung von Zahlungen abbilden möchten.

Hierfür lässt sich das Aareal Portal in vielfältiger Weise an Ihre Bedürfnisse anpassen, indem Sie beispielsweise Mitarbeitern genau die Befugnisse einräumen, Informationen einzusehen oder Zahlungen vorzunehmen, die sie für ihre Aufgaben benötigen.

Das vorliegende Handbuch für Administratoren wird Ihnen dabei helfen, die Möglichkeiten des Aareal Portals zu verstehen und zu nutzen, und es ergänzt das Handbuch für Benutzer des Aareal Portals, in dem alle Funktionen für die tägliche Arbeit von Anwendern erläutert werden. Sollten Sie sich zunächst mit der grundlegenden Bedienung und dem Funktionsumfang des Aareal Portals vertraut machen wollen, beginnen Sie bitte mit der Lektüre der Kapitel 4 und 5 im Benutzerhandbuch.

Auf den nachfolgenden Seiten finden Sie alle Informationen, die Sie benötigen, um als Administrator das Aareal Portal für Ihr Unternehmen zu konfigurieren.

In Kapitel 3 finden Sie zunächst einen schnellen Zugang zu häufigen Situationen im Alltag. Hier erhalten Sie rasch Antworten, ohne tiefer in das Handbuch einsteigen zu müssen.

Das darauffolgende Kapitel 4 gibt Ihnen einen Überblick, welche einzelnen Schritte notwendig sind, um Benutzer, imageTAN-Reader und EBICS-Berechtigungen einzurichten. Es legt einen roten Faden durch die Konfiguration des Aareal Portals. Beginnen Sie mit diesem Kapitel, wenn Sie die Konfiguration des Aareal Portals verstehen und eine Erstkonfiguration vornehmen möchten.

Die weiteren Kapitel erläutern Ihnen jeweils einzelne Aspekte der Administration:

- In Kapitel 5 erhalten Sie alle Informationen zur Einrichtung und Verwaltung von Benutzern.
- Kapitel 6 zeigt Ihnen, wie Sie effizient Zugriffsrechte definieren und Benutzern zuweisen.
- Kapitel 7 erläutert den Umgang mit imageTAN-Readern.
- In Kapitel 8 erfahren Sie, wie Sie Benutzer mit EBICS-Teilnehmern verknüpfen und ihnen damit entsprechende Berechtigungen zu den hinterlegten Konten einräumen.
- Die Einrichtung von automatischen und regelmäßigen Abrufen lesen Sie in Kapitel 9.
- Abschließend zeigt Ihnen Kapitel 10, wie Sie die Aktivitätenprotokolle nutzen können, um schnell und einfach nachvollziehen zu können, welche Benutzer Aktivitäten im Aareal Portal vorgenommen haben.

Die Aareal Bank wünscht Ihnen viel Freude bei der Verwendung des Aareal Portals.

Konventionen

Zur besseren Verständlichkeit dieses Handbuchs werden die folgenden Formatierungen durchgängig verwendet:

! ***Tipp / Hinweis**: Praktische Tipps und wichtige Hinweise werden durch ein Ausrufezeichen und kursiven Text deutlich hervorgehoben.*

Bedienbare **SCHALTFLÄCHEN** im Aareal Portal werden in Kapitälchen mit blauer Schrift dargestellt.

Bezeichnungen von Eingabefeldern, sowie Auswahloptionen werden **fett** markiert.

2. Voraussetzungen

Um das Aareal Portal als Administrator nutzen zu können, benötigen Sie einen aktiven Benutzer mit Administrationsrechten zu Ihrem Kundenzugang. Von der Aareal Bank erhalten Sie die initialen Zugangsdaten. Bitte richten Sie diesen Benutzer entsprechend den Kapiteln 2 und 3 im Benutzerhandbuch ein.

Ob Ihr Benutzerzugang mit Administrationsrechten ausgestattet ist, erkennen Sie u. a. daran, dass Ihnen nach erfolgreicher Anmeldung am Aareal Portal im Modul **ADMINISTRATION** der Menüeintrag **BENUTZER** mit diversen Funktionen zur Benutzerverwaltung zugänglich ist.

3. Schnelleinstieg: Wie kann ich …?

EINEN BENUTZER TEMPORÄR SPERREN?

Gehen Sie in das Modul **ADMINISTRATION** und öffnen Sie den Menüeintrag **BENUTZER**. Suchen Sie den entsprechenden Benutzer heraus und klicken Sie dann auf das **[+]** am Ende der Zeile. Sobald Sie die Schaltfläche **SPERREN** betätigt haben, ist der Benutzer mit sofortiger Wirkung gesperrt.

Weitere Informationen finden Sie in Kapitel 5.2 auf Seite 23.

EINEN GESPERRTEN BENUTZER WIEDER FREIGEBEN?

Um einen gesperrten Benutzer wieder freizugeben, fordern Sie für ihn neue Zugangsdaten an und lassen Sie ihn den Prozess der Erstanmeldung durchlaufen:

Gehen Sie in das Modul **ADMINISTRATION** und öffnen Sie den Menüeintrag **BENUTZER**. Suchen Sie den entsprechenden Benutzer heraus und klicken Sie dann auf das **[+]** am Ende der Zeile. Klicken Sie auf die Schaltfläche **ZUGANGSDATEN ANFORDERN** und schicken Sie dem Benutzer das Dokument zu, das Sie zum Herunterladen angeboten bekommen.

Der Benutzer kann sich nun mit diesem Schreiben neu anmelden. Der imageTAN-Reader ist weiterhin aktiviert und muss nicht neu aktiviert werden. Ebenso sind die im Schlüsselmedium hinterlegten EBICS-Schlüssel noch aktiv.

Hat sich der Benutzer dagegen selbst gesperrt, so sind aus Sicherheitsgründen auch alle EBICS-Schlüssel gelöscht worden. Erinnern Sie den Benutzer in diesem Fall bitte daran, die EBICS-Zugänge neu zu initialisieren.

Weitere Informationen finden Sie in Kapitel 5.4 und in Kapitel 6.2.3 im Benutzerhandbuch.

DAS PASSWORT ZURÜCKSETZEN?

Um einem Benutzer ein neues Passwort zu vergeben, fordern Sie für ihn neue Zugangsdaten an und lassen Sie ihn den Prozess der Erstanmeldung durchlaufen:

Gehen Sie in das Modul **ADMINISTRATION** und öffnen Sie den Menüeintrag **BENUTZER**. Suchen Sie den entsprechenden Benutzer heraus und klicken Sie dann auf das **[+]** am Ende der Zeile. Klicken Sie auf die Schaltfläche **ZUGANGSDATEN ANFORDERN** und schicken Sie dem Benutzer das Dokument zu, das Sie zum Herunterladen angeboten bekommen.

Der Benutzer kann sich nun mit diesem Schreiben neu anmelden. Der imageTAN-Reader ist weiterhin aktiviert und muss nicht neu aktiviert werden. Ebenso sind die im Schlüsselmedium hinterlegten EBICS-Schlüssel noch aktiv.

Weitere Informationen finden Sie in Kapitel 5.4.

DAS ADMINISTRATORPASSWORT ZURÜCKSETZEN?

Haben Sie das Passwort zu Ihrem Kundenzugang mit Administrationsrechten verloren oder vergessen, so wenden Sie sich bitte an Ihren Kundenberater der Aareal Bank, der Ihnen neue Zugangsdaten zukommen lässt. Ihr Schlüsselmedium bleibt in diesem Fall aktiv und kann von Ihnen weiterverwendet werden.

DIE GERÄTE-PIN ZURÜCKSETZEN?

Falls ein Benutzer sich an die selbstgewählte PIN des imageTAN-Readers nicht mehr erinnern kann, so kann er diese selbst zurücksetzen. Hierzu meldet er sich mit Kundenkennung, Benutzerkennung und Passwort am Portal an und klickt in der Loginmaske auf den Link „PIN vergessen oder gesperrt?“. Der Link ist in Abbildung 18 dargestellt.

Sollten Sie als Administrator die PIN für den Benutzer zurücksetzen wollen, oder falls der Benutzer sich auch an seine Zugangsdaten nicht mehr erinnert, gehen Sie in das Modul **ADMINISTRATION** und das Menü der **IMAGETAN-READER-VERWALTUNG**. Wiederrufen Sie nun die Lizenz des entsprechenden imageTAN-Readers mit **SCHLÜSSELMEDIUM ZURÜCKSETZEN**.

In beiden Fällen muss das Schlüsselmedium neu aktiviert und ggf. EBICS-Schlüssel neu erzeugt werden.

Weitere Informationen finden Sie in Kapitel 7.3.1.

EINEN BENUTZER FREISCHALTEN, ZU DESSEN SCHLÜSSELMEDIUM IN DER BENUTZERVERWALTUNG „WARTET AUF FREIGABE“ ANGEGEBEN IST?

Der Text „Wartet auf Freigabe“ erscheint für Benutzer, für die Sie entschieden haben, das Schlüsselmedium freigabepflichtig zu markieren und somit manuell freizuschalten.

Der Benutzer hat seinen imageTAN-Reader aktiviert und ein Schreiben zum Herunterladen angeboten bekommen, das einen Freigabecode enthält. Sobald Sie dieses Schreiben vom Benutzer erhalten haben, gehen Sie in die Benutzerverwaltung im Modul **ADMINISTRATION**, indem Sie dort den Menüeintrag **BENUTZER** auswählen. Wählen Sie dann den entsprechenden Benutzer aus und klicken Sie auf das **[+]** am Ende der Zeile. Wählen Sie nun die Schaltfläche **ÄNDERN** und wechseln Sie auf den Reiter **SCHLÜSSELMEDIUM**. Geben Sie hier den Freigabecode ein. Ist der Freigabecode korrekt, wird dies mit einem grünen Haken angezeigt. **ÜBERNEHMEN** und **SPEICHERN** Sie die Änderungen.

Bitte beachten Sie, dass Administratorzugänge durch die Aareal Bank freigeschaltet werden müssen.

Weitere Informationen und wie Sie vorgehen, falls das Schreiben verlorengegangen ist, finden Sie in Kapitel 5.5.

REAGIEREN, WENN EIN BENUTZER SEINEN IMAGETAN-READER VERLOREN HAT?

Der erste Schritt bei einem zweifelsfrei verlorengegangenen Schlüsselmedium sollte die Sperrung des Gerätes sein. Dies kann der Benutzer selbst erledigen oder Sie als Administrator übernehmen diese Aufgabe für den Benutzer.

Ein Benutzer meldet sich zur Sperrung des imageTAN-Readers mit Kundenkennung, Benutzerkennung und Passwort am Aareal Portal an und klickt in der Loginmaske auf den Link „ImageTAN-Reader sperren“. Der Link ist in Abbildung 18 dargestellt.

Auch Sie als Administrator können den imageTAN-Reader des betroffenen Benutzers deaktivieren. In beiden Fällen werden mit der Sperrung alle EBICS-Schlüssel gelöscht. Der Vorteil einer Sperrung durch Sie als Administrator besteht darin, dass der Benutzer keine neuen Zugangsdaten benötigt. Suchen Sie sich im Modul **ADMINISTRATION** und im Menü **BENUTZER** den betroffenen Benutzer heraus und **ÄNDERN** Sie diesen. Wechseln Sie nun auf den Reiter Schlüsselmedium und klicken Sie auf die Schaltfläche mit dem kleinen Pfeil entgegen des Uhrzeigersinns.

Weitere Informationen finden Sie in Kapitel 7.3.3.

HERAUSFINDEN, ZU WELCHEM BENUTZER EIN IMAGETAN-READER GEHÖRT?

Öffnen Sie das Menü **Einstellungen** am imageTAN-Reader, indem Sie in ausgeschaltetem Zustand den Ein-/Aus-Knopf am oberen Ende des Gerätes mindestens 3 Sekunden gedrückt halten. Wählen Sie dann den Punkt Aktivierungen aus und lassen Sie sich die Lizenz anzeigen.

Wechseln Sie nun im Aareal Portal in das Modul Administration und den Menüpunkt **IMAGETAN-READER-VERWALTUNG** und geben Sie im Eingabefeld die Lizenz aus dem Gerät ein.

Der mit dem imageTAN-Reader verknüpfte Benutzerzugang wird nun angezeigt. Sollte kein Benutzerzugang gefunden werden, so wurde die Lizenz bereits widerrufen.

Weitere Informationen finden Sie in Kapitel 7.3.4.

SPRACHEINSTELLUNGEN FÜR AUTOMATISCH GENERIERTE NACHRICHTEN?

Um die Spracheinstellungen für automatisch generierte Nachrichten für alle Benutzer zu ändern, gehen Sie in das Modul **ADMINISTRATION** und das Menü **BENUTZER**. Ändern Sie die Sprache mit Hilfe der Auswahlbox „Sprache“.

Weiter Informationen finden Sie in Tabelle 1 in Kapitel 5.

4. In wenigen Schritten zum einsatzbereiten Aareal Portal

Im folgenden Kapitel erhalten Sie einen Überblick über die administrativen Tätigkeiten im Aareal Portal. Lesen Sie dieses Kapitel insbesondere dann aufmerksam, wenn Sie mit der Administration des Aareal Portals noch nicht vertraut sind und zunächst ein Gesamtverständnis erlangen möchten.

Beginnen Sie mit der Administration des Aareal Portals, indem Sie für Ihre Benutzer Zugänge einrichten und ihnen die zur Anmeldung benötigten imageTAN-Reader zur Verfügung stellen.
Wie Sie diese Schritte durchführen, erfahren Sie in den Kapiteln 5.1 und 5.4 weiter unten im Handbuch. Um ein tieferes Verständnis der Benutzerverwaltung zu erhalten, sei das gesamte Kapitel 5 als Lektüre empfohlen.

Ein Benutzer kann, sobald er diese Schritte durchlaufen hat und sich am Aareal Portal anmelden kann, auf alle Daten und Seiten im Aareal Portal zugreifen, auf die er entsprechend seiner ihm zugeordneten Module und Rollen bzw. entsprechend den gegebenenfalls hinterlegten Konteneinschränkungen berechtigt ist. Insbesondere kann er Zahlungsdaten und Kontoumsätze einsehen, die im Aareal Portal gespeichert sind, beispielsweise, weil sie bereits von einem anderen Portalbenutzer vom Bankrechner abgerufen wurden. Demzufolge kann auch ein Benutzer ohne Zeichnungsbefugnis solche Daten einsehen, sofern für ihn keine entsprechenden Kontoeinschränkungen hinterlegt sind.

Soll er darüber hinaus selbst Umsatzdaten abrufen oder Zahlungsaufträge an Banken übertragen oder freigeben können, so benötigt er für die jeweilige Bank eine entsprechende Berechtigung. Diese wird in Form von EBICS-Teilnehmerkennungen erteilt und einzelnen Benutzern zugewiesen. Die EBICS-Teilnehmerdaten erhalten Sie vom Bankberater der jeweiligen Bank, auf die Sie Benutzer berechtigen möchten.
Einen Überblick über EBICS-Berechtigungen erhalten Sie in Kapitel 5.2 des Benutzerhandbuchs.

Möchten Sie neben Ihren Konten bei der Aareal Bank auch Konten anderer Banken im Aareal Portal verwalten, so müssen Sie für die jeweilige Bank einen Bankparameter einrichten. Der Bankparameter beschreibt die Verbindung zum Kernbanksystem der jeweiligen Bank und bildet somit die Basis für die sichere Kommunikation zwischen dem Aareal Portal und Ihrer Bank.
Der Bankparameter zu Ihren Konten der Aareal Bank ist bereits für Sie eingerichtet.

- Prüfen Sie, ob Ihr Kundenzugang für die Fremdbankanbindung freigeschaltet ist. Tabelle 1 in Kapitel 5 hilft Ihnen dabei.
  Falls Ihr Zugang nicht freigeschaltet ist, Sie dies jedoch wünschen, sprechen Sie bitte Ihren Kundenberater der Aareal Bank an.
- Erstellen Sie einen Bankparameter für jede der Banken, mit denen Sie im Aareal Portal arbeiten möchten. Diese Funktion ist im Benutzerhandbuch in Kapitel 6.2.1 detailliert erläutert.

Jeder Benutzer, der wie oben beschrieben, Umsatzdaten vom Bankrechner abholen oder Zahlungsaufträge freigeben möchte, benötigt eine EBICS-Teilnehmer-ID und muss

diese mit Hilfe seines imageTAN-Readers initialisieren, d. h. die für die Kommunikation benötigten Schlüssel erzeugen.

- Weisen Sie jedem Benutzer, der eine EBICS-Berechtigung erhalten soll, eine EBICS-Teilnehmer-ID zu. Kapitel 8 beschreibt die einzelnen Schritte dafür. Alternativ kann ein Portalbenutzer diesen Schritt für seinen eigenen Benutzerzugang auch selbst übernehmen.
- Abschließend muss jeder Benutzer seine EBICS-Teilnehmer-ID initialisieren. Dies ist im Benutzerhandbuch in Kapitel 6.2.3 beschrieben.

Ihre Benutzer sind nun eingerichtet und können mit dem Aareal Portal arbeiten.

Sie haben bislang bereits erfahren, dass es verschiedene Bereiche gibt, die in der Administration des Aareal Portals eine spezifische Rolle spielen. Nachfolgend sind diese nochmals aufgeführt:

- Über einen Benutzerzugang erhält ein Mitarbeiter Zugang zum Aareal Portal. Er kann die bereits abgerufenen Daten entsprechend seinen Berechtigungen einsehen, aber noch nicht mit dem Rechner einer Bank kommunizieren. Für den Zugang zum Aareal Portal benötigt er einen imageTAN-Reader.
  Alles Wissenswerte zu den Benutzerzugängen erfahren Sie in Kapitel 5.

- Der imageTAN-Reader wird von jedem Benutzer benötigt, um sicheren Zugang zum Aareal Portal zu erhalten. Zusätzlich dient er als Schlüsselmedium für die Kommunikation mit dem Bankrechner, beispielsweise um Zahlungen freizugeben, oder um Umsatzdaten abzurufen.
  Genauer wird auf den imageTAN-Reader in Kapitel 7 eingegangen.

- Auf welche Seiten im Aareal Portal ein Benutzer Zugang hat, wird über definierbare Rollen und über die Auswahl der Module gesteuert, die dem jeweiligen Benutzer zugewiesen werden. Details dazu erfahren Sie in Kapitel 6.

- Möchten Sie neben den Konten der Aareal Bank auch Konten weiterer Banken im Aareal Portal verwalten, so müssen Sie für jede Bank einen Bankparameter einrichten. Dieser bildet die Basis für die Kommunikation mit dem Bankrechner über EBICS. Wie Sie Bankparameter einrichten, lesen Sie im Benutzerhandbuch in Kapitel 6.2.1.

- Schließlich benötigt jeder Benutzer, der über EBICS Aufträge an Banken senden möchte, eine EBICS-Teilnehmer-ID, die er im nächsten Schritt initialisieren muss. Auf die Zuordnung von EBICS-Teilnehmer-IDs zu Benutzern geht Kapitel 8 detailliert ein. Die Initialisierung von EBICS-Teilnehmer-IDs wird im Benutzerhandbuch in Kapitel 6.2.3 erläutert.

5. Benutzer einrichten

Die Entscheidung darüber, wer in Ihrem Unternehmen Zugang zum Aareal Portal hat und bestimmte Aktionen ausführen darf, ist sicher das zentrale Anliegen für Sie als Administrator.

In diesem Kapitel erfahren Sie, wie Sie neue Benutzer zum Aareal Portal hinzufügen, deren Rechte festlegen, Benutzer zeitweise sperren oder löschen. Ebenso erfahren Sie in diesem Kapitel, wie sie Benutzern, die ihr Passwort oder ihren imageTAN-Reader verloren haben, wieder den Zugang zum Aareal Portal ermöglichen.

Das Aareal Portal kennt drei Arten von Zugängen:

- Ein *Benutzer* ist eine Person, die sich mit eigenen Zugangsdaten am Aareal Portal anmelden kann.

- Ein *Administrator* ist ein Benutzer mit zusätzlichen Rechten zur Administration des Aareal Portals. Er kann neue Benutzerzugänge anlegen und diese sperren oder neue Zugangsdaten vergeben. Er kann ihnen Rechte vergeben oder sie mit Einschränkungen versehen. Zusätzlich kann er über das Aktivitätenprotokoll Vorgänge im Aareal Portal nachvollziehen und auf einzelne Benutzer zurückführen.

- Ein *Administrator der Aareal Bank* pflegt Ihren Kundenzugang und steht Ihnen unterstützend für bestimmte Tätigkeiten zur Verfügung. Er kann Ihnen beispielsweise weitere Benutzer mit Administrationsrechten vergeben oder Ihren Unternehmensnamen ändern. Manche Tätigkeiten müssen zwingend durch diesen Administrator vorgenommen oder bestätigt werden.

Um Benutzer anzulegen oder Änderungen vorzunehmen, öffnen Sie das Modul **ADMINISTRATION** in der oberen Menüleiste und wählen Sie den Menüeintrag **BENUTZER**. Sie sehen die Maske zur Verwaltung von Benutzern, wie Sie in Abbildung 1 dargestellt ist.

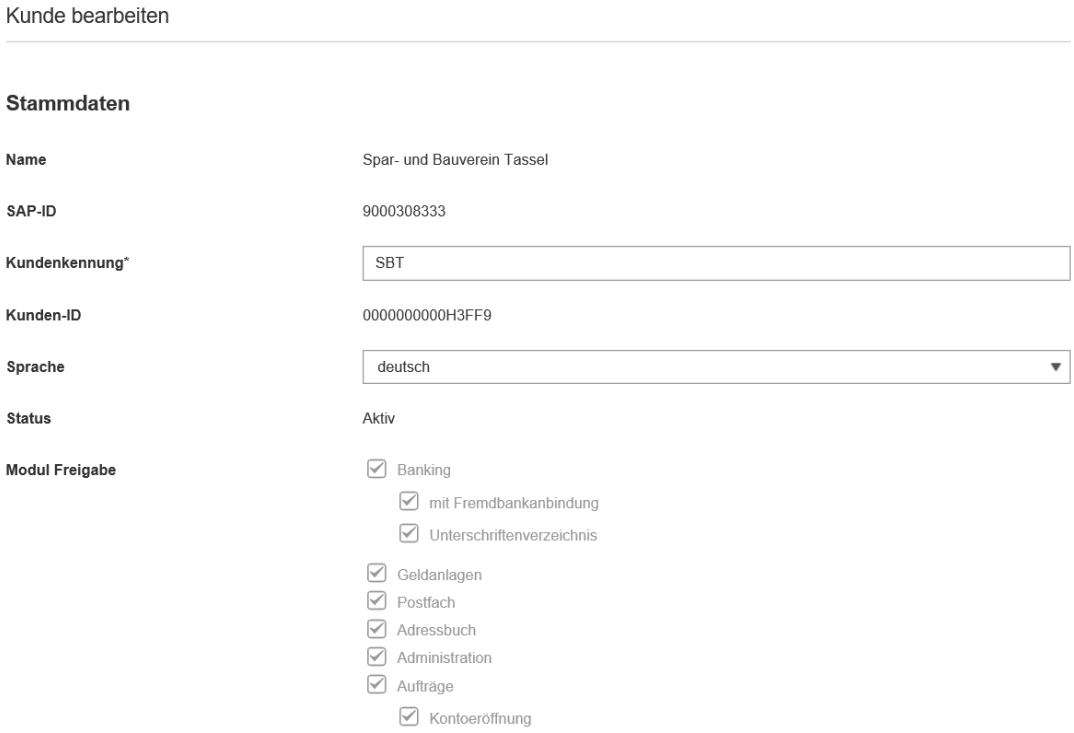

Abbildung 1: Darstellung der Stammdaten in der Benutzerverwaltung

Die Seite ist in zwei Bereiche unterteilt. Im oberen Bereich finden Sie die **Stammdaten**, also Informationen rund um Ihren Kundenzugang bei der Aareal Bank. Hier sehen Sie die folgenden Informationen:

Name	Der Name Ihres Unternehmens. Dieser wird beim Anlegen Ihres Kundenzugangs entsprechend Ihrer Angaben von der Aareal Bank vergeben. Sollten Sie ihn anpassen müssen, wenden Sie sich bitte an Ihren Kundenberater.
SAP-ID	Die 10-stellige SAP-ID verknüpft zusammen mit der Kunden-ID Ihren Kundenzugang mit dem Kernbanksystem der Aareal Bank.
Kundenkennung	Die für Sie frei wählbare Kundenkennung identifiziert Ihren Kundenzugang eindeutig im Aareal Portal. Sie benötigen Ihre Kundenkennung beispielsweise, um sich am Aareal Portal anzumelden. Sie können die Kundenkennung jederzeit ändern. Bitte denken Sie daran, die neue Kennung allen Benutzern mitzuteilen, da diese sich sonst nicht mehr am Aareal Portal anmelden können. Eine Änderung ist nach der Speicherung sofort wirksam. Bei der Wahl einer neuen Kundenkennung können Sie neben Ziffern und allen im deutschen Sprachraum üblichen Buchstaben die folgenden Sonderzeichen verwenden: _ @ ! $ % & / ( ) = ? - | > < Die Kundenkennung kann bis zu 15 Zeichen umfassen und darf im Aareal Portal noch nicht durch einen anderen Kunden genutzt werden. Bitte **SPEICHERN** Sie Ihre Eingabe am unteren Ende der Seite.

Kunden-ID	Die Kunden-ID verknüpft zusammen mit der SAP-ID Ihren Kundenzugang mit dem Kernbanksystem der Aareal Bank.
Sprache	Die hier eingestellte Sprache bezieht sich auf die Sprache von automatisch generierten Nachrichten für alle Benutzer eines Kunden. Dies betrifft Nachrichten im Postfach, den sonstigen Protokollen und dem Aktivitätenprotokoll und ist unabhängig von der benutzerspezifischen Einstellung der Sprache für die Oberfläche (Siehe Benutzerhandbuch).
Status	Dieses Feld zeigt den aktuellen Status Ihres Kundenzugangs an: aktiv oder inaktiv. Bei einer Deaktivierung des Kundenzugangs werden automatisch alle Benutzer gesperrt. Daher werden auch Sie als Kundenadministrator nie den Zustand „Inaktiv“ zu sehen bekommen. Denken Sie nach einer Reaktivierung durch Ihren Aareal Kundenberater bitte daran, alle gesperrten Benutzer wieder freizuschalten, indem Sie für jeden Benutzer neue Zugangsdaten anfordern (s. Kapitel 5.4).
Modul Freigabe	Hier sehen Sie alle Module, die für Sie im Aareal Portal freigeschaltet sind. Sprechen Sie Ihren Aareal Kundenberater an, um die Auswahl der aktivierten Module anzupassen. Eine Übersicht über alle im Aareal Portal zur Verfügung stehenden Module finden Sie im Benutzerhandbuch in Kapitel 4.2 auf Seite 15. Ist für Sie die Funktion zur Anzeige und Verwendung von Konten anderer Banken im Aareal Portal freigeschaltet, so sehen Sie hier das Stichwort **Fremdbankanbindung**.

Tabelle 1: Stammdaten des Kundenzugangs

Unterhalb der Stammdaten sind in der Tabelle **Benutzer des Kunden** alle aktiven und beendeten Benutzer Ihres Kundenzugangs aufgelistet. Hier können Sie neue Benutzer anlegen, sperren oder löschen (Status: „Beendet“), Passwörter zurücksetzen, und für Benutzer über Rollen, Module und Kontoeinschränkungen verfügen.

! ***Hinweis**: Bitte denken Sie bei Änderungen an einem bestehenden Benutzer oder bei der Neuanlage von Benutzern daran, diese mit der Schaltfläche* **SPEICHERN** *am unteren Ende der Tabelle zu speichern. Andernfalls gehen Ihre Änderungen verloren.*

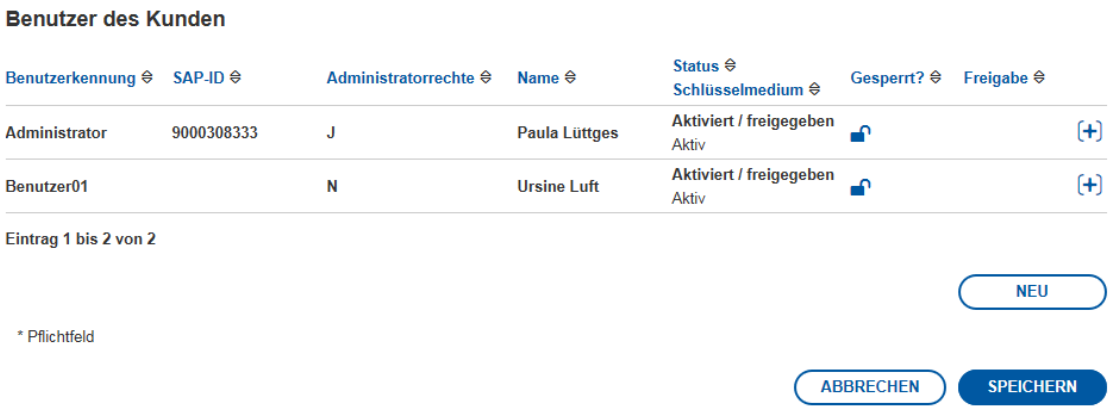

Abbildung 2: Benutzer eines Kundenzugangs

Die **Benutzerkennung** identifiziert einen Benutzer innerhalb Ihres Kundenzugangs eindeutig. Mit Hilfe der Benutzerkennung, der von Ihnen oben festgelegten Kundenkennung und dem vom Benutzer selbst gewählten Passwort meldet sich der Benutzer am Aareal Portal an. Die Benutzerkennung taucht ebenso an anderen Stellen im Aareal Portal auf, wie z. B. in den Protokollen.

Eine **SAP-ID** ist nur für Benutzer mit Administrationsrechten hinterlegt. Ob diese vorhanden sind, erkennen Sie an einem „J“ in der Spalte **Administratorrechte**. Um einen neuen Benutzer mit Administrationsrechten anzulegen, wenden Sie sich bitte an Ihren Kundenberater der Aareal Bank. Dieser kann für Sie auch einem bereits vorhandenen Benutzer Administrationsrechte vergeben oder diese wieder entziehen. Für die Vergabe von Administrationsrechten wird Ihr Kundenberater eine SAP-ID und die vollständige Anschrift des Benutzers benötigen.

In der Spalte **Name** sehen Sie den vollständigen Namen des Benutzers.

Die nächste Spalte zeigt Ihnen den **Status** des Benutzerzugangs und des **Schlüsselmedium**s des jeweiligen Benutzers an.

Folgende Zustände können am Benutzerzugang auftreten:

Angelegt	Ein Benutzerzugang wurde neu angelegt. Es wurden noch keine Zugangsdaten erstellt und versendet.
Zugangsdaten sind versendet / erstellt	Für diesen Benutzerzugang wurden nach der Neuanlage des Benutzers, auf Grund einer Sperre, eines vergessenen Passwortes oder anderen Gründen Zugangsdaten angefordert. Der Benutzer hat sich mit seinen initialen Zugangsdaten noch nicht angemeldet.
Aktiviert / freigegeben	Dies ist der Grundzustand eines aktivierten Benutzer-zugangs. Der Benutzer kann im Portal arbeiten.
Gesperrt	Der Zugang des Benutzers wurde auf Grund einer dreifachen Falscheingabe des Passworts oder der TAN, oder durch das bewusste Setzen einer Sperre gesperrt. Je nach Ursache der

	Sperre muss der imageTAN-Reader neu aktiviert, und es müssen neue EBICS-Schlüssel erzeugt werden.
Beendet	Ein beendeter Benutzer ist auf Dauer deaktiviert, eine Reaktivierung ist nicht möglich. Der Benutzer wird zur Nachvollziehbarkeit weiterhin in der Tabelle angezeigt.

Tabelle 2: Mögliche Status eines Benutzerzugangs

Folgende Zustände können am Schlüsselmedium auftreten:

Status	Beschreibung
Aktiv	Das Schlüsselmedium wurde aktiviert und ist mit dem Benutzerzugang verknüpft.
Wartet auf Freigabe	Das Schlüsselmedium wurde vom Benutzer aktiviert und wartet auf Freigabe durch den Administrator. Geben Sie den Freigabecode ein, den Sie vom Benutzer zurückerhalten. Weitere Informationen hierzu erhalten Sie in Kapitel 5.5. Dieser Status wird nur verwendet, wenn die Auswahl „Schlüsselmedium freigabepflichtig“ im Reiter **Schlüsselmedium** bei der Anlage des Benutzers gewählt wurde.
Unbekannt	Das Schlüsselmedium wurde noch nicht aktiviert. Es ist kein Schlüsselmedium an den Benutzerzugang gebunden oder die Verbindung wurde wieder aufgehoben, beispielsweise weil sich der Benutzer gesperrt hatte.

Tabelle 3: Mögliche Status des Schlüsselmediums

Die Spalte „**Gesperrt?**“ zeigt Ihnen an, ob ein Benutzer gegenwärtig gesperrt ist oder nicht. Gesperrte Benutzer werden durch ein Symbol eines roten, verschlossenen Schlosses dargestellt. Nicht gesperrte Benutzer erkennen Sie an einem geöffneten, blauen Schloss.

Mehr über das Sperren und Entsperren von Benutzern erfahren Sie in Kapitel 5.2.

Freigabe von Benutzern

Werden Benutzer durch einen Administrator der Aareal Bank angelegt oder von ihm Änderungen vorgenommen, so müssen diese nach dem 4-Augen-Prinzip von einem zweiten Administrator der Aareal Bank freigegeben werden. Dieses Verfahren stellt sicher, dass Fehler in der Administration vermieden werden.
Steht die Zweitfreigabe noch aus, erscheint in der Spalte **Freigabe** der Hinweistext „In Freigabe“. Zusätzlich wird die gesamte Zeile grau hinterlegt. Änderungen am Benutzer werden erst dann wirksam, wenn auch die zweite Freigabe erfolgt ist.

Als Administrator Ihres Kundenzugangs unterliegen Sie in Bezug auf die Freischaltung Ihrer Mitarbeiter nicht dem 4-Augen-Prinzip. Änderungen an Benutzern, die Sie selbst durchführen, werden direkt nach der Betätigung der Schaltfläche **SPEICHERN** wirksam.

Abbildung 3: Aktionen zum Sperren, Löschen, Ändern und Anfordern neuer Zugangsdaten

Über das **[+]** am Zeilenende eines Benutzereintrags erhalten Sie Zugang zu den Aktionen, die Sie zum jeweiligen Benutzer durchführen können. Dies sind im Einzelnen:

- Sie können einen Benutzer temporär **SPERREN**. Seine Einstellungen und hinterlegten Daten einschließlich eventuell vorhandener EBICS-Schlüssel bleiben dabei erhalten. Eine Sperre ist sofort wirksam. Um eine Sperre wieder aufzuheben, benutzen Sie bitte die Schaltfläche **ZUGANGSDATEN ANFORDERN** und durchlaufen Sie den Freigabeprozess.
- Durch die Schaltfläche **LÖSCHEN** wird der Benutzer gelöscht.
  Aus Gründen der Nachvollziehbarkeit bleibt ein gelöschter Benutzer dauerhaft in der Tabelle **Benutzer des Kunden** im Status „Beendet“ sichtbar. Eine Reaktivierung des Benutzers ist nicht möglich.
  Falls der Benutzer noch mit einem aktiven imageTAN-Reader verbunden ist, so wird die zum imageTAN-Reader gehörende Lizenz automatisch freigegeben. Der imageTAN-Reader ist somit deaktiviert und kann von einem neuen Benutzer aktiviert und verwendet werden.
- Mit Hilfe der Schaltfläche **ÄNDERN** können Sie jederzeit alle Daten, Rechte, Einschränkungen, usf. eines Benutzers anpassen.
  Bitte beachten Sie, dass Änderungen am Benutzer erst übernommen werden, wenn Sie nach Betätigung der Schaltfläche **OK** im Änderungsdialog auch die Schaltfläche **SPEICHERN** betätigt haben. Falls Sie dies vergessen, werden die vorgenommenen Änderungen verworfen und Sie müssen sie gegebenenfalls neu eingeben.
- Über die Schaltfläche **ZUGANGSDATEN ANFORDERN** können Sie einen Benutzer jederzeit ein neues Passwort setzen lassen, beispielsweise nachdem dieser von Ihnen neu angelegt oder gesperrt worden war. Weitere Informationen hierzu erhalten Sie in Kapitel 5.4.

5.1. Einen neuen Benutzer anlegen oder einen bestehenden Benutzer ändern

Um einen neuen Benutzer anzulegen, gehen Sie im Modul **ADMINISTRATION** auf den Menüeintrag **BENUTZER** und klicken Sie auf die Schaltfläche **NEU** am unteren Ende der Seite.

Falls Sie Daten, Rollen oder Einschränkungen an einem bestehenden Benutzer verändern möchten, öffnen Sie ebenfalls diese Seite zur Verwaltung von Benutzern über **ADMINISTRATION ▶ BENUTZER**. Wählen Sie dann aus der Tabelle einen bestehenden Benutzer aus, öffnen Sie das Aktionsmenü über **[+]** und betätigen Sie die Schaltfläche

ÄNDERN. Alternativ können Sie auch einfach in die Zeile des zu bearbeitenden Benutzers klicken.

Es öffnet sich der Dialog **Benutzer bearbeiten** mit vier Reitern. Im Folgenden wird stellvertretend auf den Dialog zum Anlegen eines neuen Benutzers eingegangen. Eingaben zur Bearbeitung eines Benutzers erfolgen analog, auf Stellen mit Abweichungen wird entsprechend hingewiesen.

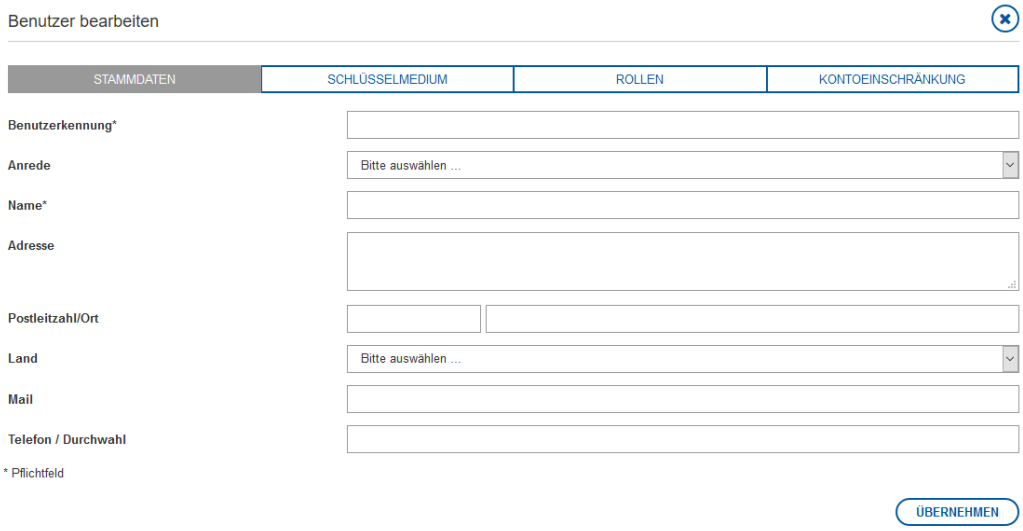

Abbildung 4: Einen neuen Benutzer anlegen – Eingabe der Stammdaten

Geben Sie im Reiter **Stammdaten** zunächst die personenbezogenen Daten des Benutzers an:

Die **Benutzerkennung** identifiziert diesen Benutzer eindeutig in Ihrem Kundenzugang des Aareal Portals. Er wird sich mit Hilfe dieser Benutzerkennung, der Kundenkennung und seinem Passwort am Aareal Portal anmelden. Aber auch im Rahmen der Protokollierung oder bei der Zuordnung von Benutzern zu imageTAN-Readern wird die Benutzerkennung eine Rolle spielen.

Sie sind in der Wahl der Benutzerkennung frei. Eine Benutzerkennung muss eindeutig sein, d.h. sie darf noch nicht in Ihrem Kundenzugang vorhanden sein. Insgesamt stehen Ihnen bis zu 100 Zeichen zur Verfügung.

! **Hinweis**: *Es hat sich als sinnvoll erwiesen, Benutzerkennungen an Hand einer aus Ihrer Sicht hilfreichen Systematik zu vergeben, die Sie schnell auf den jeweiligen Benutzer schließen lässt. Wählen Sie eine einfach zu merkende Benutzerkennung, da der Benutzer diese bei jeder Anmeldung eingeben muss.*

Geben Sie unter **Name** den vollen Namen des Benutzers an. Dieser Name wird an verschiedenen Stellen im Aareal Portal verwendet, um den Benutzer anzusprechen oder ihn zu identifizieren. So erscheint der Name beim angemeldeten Benutzer oben rechts im Portal, in den verschiedenen Protokollen, aber auch im Brief zur Freischaltung des Benutzerzugangs.

Die Angaben zu **Benutzerkennung** und **Name** müssen zu einem Benutzer mindestens gemacht werden, anschließend können Sie den neuen Benutzer mit der Schaltfläche **ÜBERNEHMEN** in die Benutzerübersicht aufnehmen. Klicken Sie dann, sobald sich der Dialog geschlossen hat, unbedingt auf die Schaltfläche **SPEICHERN**, um den Vorgang abzuschließen und den neuen Benutzer anzulegen.

In den meisten Fällen wird es hilfreich für Sie sein, die restlichen Angaben zu vervollständigen. So verfügen Sie über aktuelle Daten, wenn Sie oder andere Administratoren den Benutzer später kontaktieren müssen, z. B. um Hilfestellung geben zu können.

Die vollständig ausgefüllte postalische **Adresse** inkl. **Postleitzahl**, **Ort** und **Land** wird in den Freischaltbrief übernommen. Möchten Sie den Brief per Post verschicken, so ist es hilfreich, wenn die gültige Anschrift hier hinterlegt ist.

Eine gültige **Mail**-Adresse ist notwendig, damit der Benutzer Benachrichtigungen im Postfach einrichten kann.

Auf dem nächsten Reiter **Schlüsselmedium** können Sie Einstellungen zum Schlüsselmedium des Benutzers vornehmen.

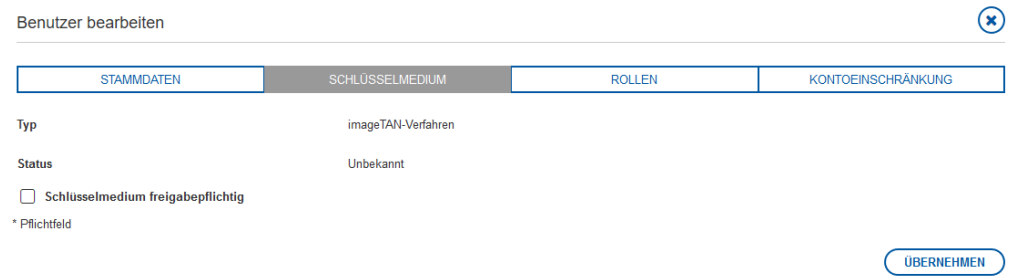

Abbildung 5: Einen neuen Benutzer anlegen – Schlüsselmedium hinterlegen

Der **Typ** „imageTAN-Verfahren“ ist fest vorgegeben und beschreibt das Anmeldeverfahren mit Hilfe des Schlüsselmediums imageTAN-Reader.

Am **Status** sehen Sie einen der Werte aus Tabelle 3: Aktiv, Wartet auf Freigabe oder Unbekannt. Dieser Wert wird Ihnen auch in der Tabelle **Benutzer des Kunden** in der Spalte **Schlüsselmedium** angezeigt.

Setzen Sie den Haken bei **Schlüsselmedium freigabepflichtig**, wenn Sie den Benutzer von Hand freischalten möchten. Der Benutzer erhält dann ein Schreiben mit einem Freischaltcode zum Herunterladen angeboten, sobald er seinen imageTAN-Reader aktiviert hat, und wird aufgefordert dieses an Sie weiterzuleiten. Eine Anmeldung ist für ihn erst möglich, nachdem der Code von Ihnen verifiziert wurde.
Dieser zusätzliche Schritt zur Freischaltung von Benutzern ist ausführlich in Kapitel 5.5 beschrieben.

! **Hinweis**: *Das Schlüsselmedium für einen Administratorzugang unterliegt immer der Freigabepflicht. Die Freigabe muss durch die Aareal Bank erfolgen.*

Wurde ein Schlüsselmedium bereits aktiviert und freigegeben, dann erhalten Sie auf der rechten Seite des Dialogs die Möglichkeit, die Aktivierung zu widerrufen. Abbildung 6 veranschaulicht dies. Mit Klick auf das Icon mit dem Pfeil entgegen der Uhrzeigerrichtung setzen Sie das Schlüsselmedium zurück und deaktivieren alle daran gebundenen digitalen Schlüssel aller Banken. Sie müssen den Benutzer neu aktivieren, damit er sich wieder am Aareal Portal anmelden kann.

! **Hinweis**: *Um das Schlüsselmedium eines Administratorzugangs zu widerrufen, wenden Sie sich bitte an Ihren Kundenberater der Aareal Bank.*

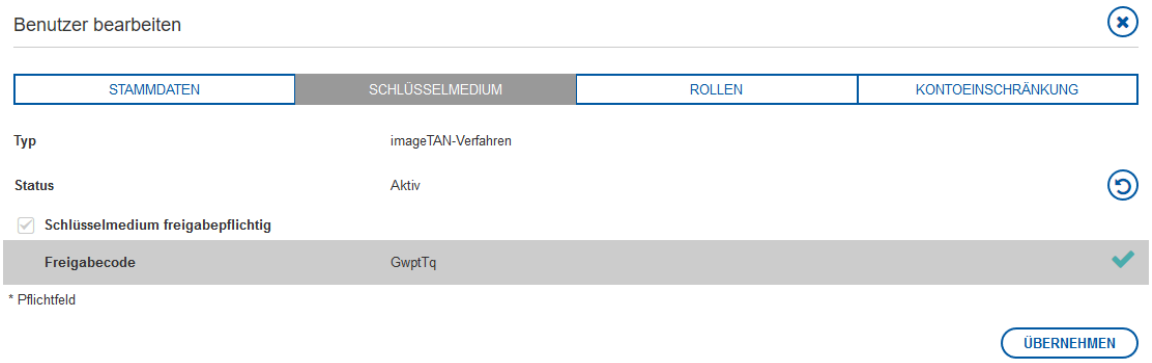

Abbildung 6: Ein aktiviertes Schlüsselmedium mit Möglichkeit zum Widerruf

Der nächste Reiter **Rollen** lässt Sie festlegen, welche Informationen der Benutzer einsehen oder bearbeiten kann.

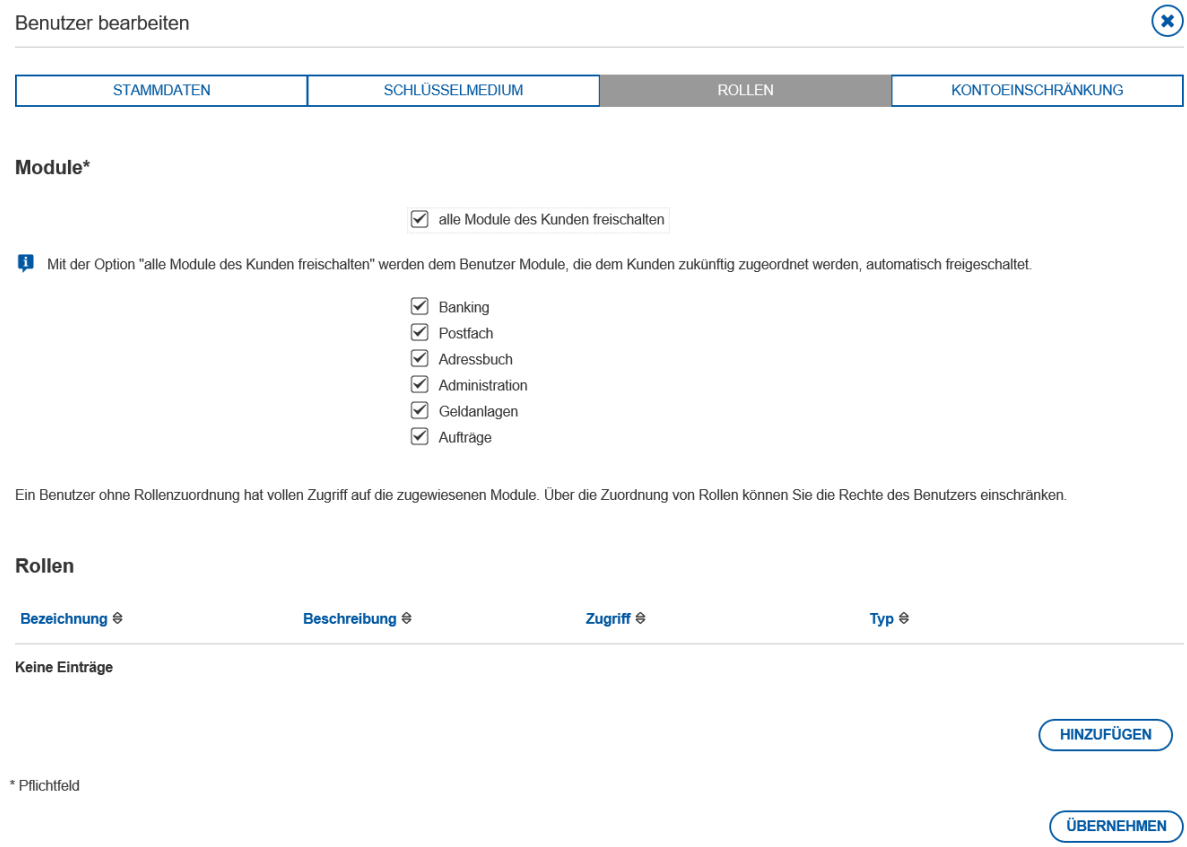

Abbildung 7: Einen neuen Benutzer anlegen – Module auswählen und Rollen festlegen

In der Standardeinstellung erhält der Benutzer Zugang zu allen derzeit freigeschalteten Modulen des Kunden. Wie Sie in Abbildung 7 sehen, sind alle aktuell verfügbaren Module vorausgewählt. Falls Sie den Benutzer automatisch auch für alle Module freischalten wollen, die zukünftig im Aareal Portal vorhanden und für Sie aktiviert sein werden, so setzen Sie den Haken bei **alle Module des Kunden freischalten**. Dies erspart Ihnen zukünftig die Änderung aller Benutzer, die für den Gesamtumfang des Aareal Portals berechtigt werden sollen.

Wenn Sie keine weiteren Änderungen vornehmen, kann der Benutzer auf alle Funktionen aller von Ihnen gewählten Module zugreifen. Für den Benutzer nicht erforderliche Module können Sie durch Entfernen des Häkchens abwählen. Dem Benutzer werden diese Module dann im Aareal Portal nicht angezeigt. Möchten Sie die für den Benutzer verfügbaren Funktionen weiter einschränken, so können Sie dem Benutzer Rollen zuweisen.

! **Hinweis**: *Für Benutzer ohne Administrationsrechte (vgl. Abbildung 2) beinhaltet das Modul* **ADMINISTRATION** *Funktionen zum Ändern des eigenen Passwortes, zur Verwaltung eigener EBICS-Schlüssel, von Abrufen im Abrufmanager und zur Ansicht der Protokolle. Benutzer erhalten hierüber nicht automatisch Zugang zu administrativen Funktionen wie der Benutzerverwaltung, der Verwaltung von Rollen und Rechten oder der imageTAN-Reader. Diese Funktionen sehen nur mit Administrationsrechten ausgestattete Benutzer.*

Klicken Sie hierfür auf die Schaltfläche **HINZUFÜGEN** und wählen Sie eine oder mehrere Rollen aus, die Sie dem Benutzer zuweisen möchten.

Der Funktionsumfang, der einem Benutzer im Aareal Portal zur Verfügung steht, ergibt sich aus der Addition aller Berechtigungen aus allen ihm zugewiesenen Rollen. Definiert beispielsweise eine Rolle, dass ein Benutzer auf das Postfach lesend zugreifen darf, und besagt gleichzeitig eine weitere ihm zugewiesene Rolle, dass er das Postfach schreibend nutzen darf, so gilt immer das höhere, in diesem Fall schreibende Recht.

Wie Sie weitere Rollen anlegen, erfahren Sie in Kapitel 6.1.

Im letzten Reiter **Kontoeinschränkung** können Sie hinterlegen, auf welche Konten ein Benutzer zugreifen darf. Details zu den Konfigurationsmöglichkeiten entnehmen Sie bitte Kapitel 6.2.

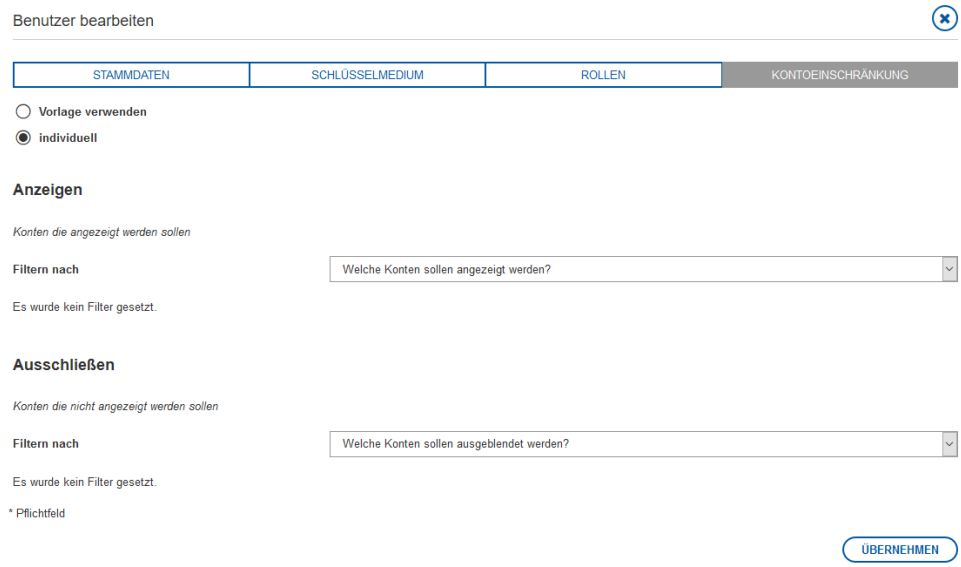

Abbildung 8: Einen neuen Benutzer anlegen – Kontoeinschränkungen festlegen

Sobald Ihre Eingaben vollständig sind, können Sie die Angaben zum Benutzer mit der Schaltfläche **ÜBERNEHMEN** in die Benutzerverwaltung übernehmen. Vergessen Sie nicht die Änderungen anschließend zu **SPEICHERN**, um den Vorgang abzuschließen.

Der neue Benutzer ist nun angelegt und wird im Zustand „Angelegt“ angezeigt. Damit er sich anmelden kann, benötigt er die initialen Zugangsdaten. Bitte folgen Sie den Anweisungen in Kapitel 5.4, um ihm diese zur Verfügung zu stellen.

5.2. Benutzer sperren

Gesperrte Benutzer können sich nicht am Aareal Portal anmelden und erhalten auf der Anmeldeseite einen entsprechenden Hinweis.

Um einen Benutzer zu sperren, benutzen Sie die Schaltfläche **SPERREN** unterhalb des jeweiligen Benutzereintrags. Möchten Sie ihn wieder entsperren, müssen Sie mit Hilfe der Schaltfläche **ZUGANGSDATEN ANFORDERN** den Freischaltungsprozess durchlaufen,

den Sie auch bei der Neuanlage von Benutzern verwendet haben. Selbstverständlich bleiben während der Sperrung eines Benutzers dessen Einstellungen und hinterlegte Daten vollständig erhalten.

! **Hinweis**: *Das Sperren eines Benutzers benötigt kein zusätzliches* **SPEICHERN** *der Änderung, die Aktion ist sofort wirksam. Sollte der Benutzer gerade angemeldet sein, so wird seine Session beendet und er damit abgemeldet.*

! **Hinweis**: *Sie können auch Ihren eigenen Administratorzugang sperren. Sofern Sie keinen weiteren Administratorzugang angelegt haben, ist es Ihnen vorübergehend nicht mehr möglich das Aareal Portal zu verwalten. Für eine Freischaltung wenden Sie sich bitte in diesem Fall an Ihren Kundenberater der Aareal Bank.*

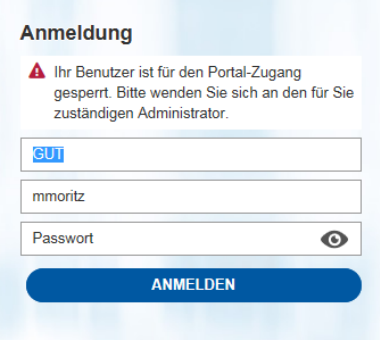

Abbildung 9: Hinweistext eines gesperrten Benutzers

Aus Sicherheitsgründen kennt das Aareal Portal zwei Abstufungen von Sperren:

Ein Benutzer, der sein persönliches Passwort dreimal falsch eingibt, oder dem neue Zugangsdaten zugeschickt werden – beispielsweise, weil er sein Passwort vergessen hat – kann direkt nach dem Setzen eines neuen Passworts regulär weiterarbeiten. Sein imageTAN-Reader bleibt aktiviert.

Wurde ein Benutzer auf Grund einer der nachfolgend aufgeführten Aktivitäten gesperrt, so wird zum einen die Lizenz des imageTAN-Readers widerrufen und dieser somit deaktiviert. Zum anderen werden die Schlüssel seiner EBICS-Teilnehmer-ID gelöscht. Der Benutzer muss daher nach der Vergabe eines neuen Passworts die entsprechenden Schritte zur Aktivierung des imageTAN-Readers und zum Erstellen neuer EBICS-Schlüssel erneut durchlaufen.

Aktionen, die zur Deaktivierung der imageTAN-Reader-Lizenz und der EBICS-Schlüssel führen, sind:

- Die dreifache Falscheingabe der TAN
- Das Klicken auf den Link **IMAGETAN-READER SPERREN** im Anmeldebildschirm durch den Benutzer
- Die Deaktivierung des Readers in der imageTAN-Reader-Verwaltung

5.3. Einen weiteren Administrator anlegen lassen

Es ist aus verschiedenen Gründen sinnvoll, die administrativen Tätigkeiten auf mehrere Personen zu verteilen. Bessere Erreichbarkeit, Verteilung von Arbeitslast oder die Möglichkeit der Vertretung im Urlaubs- oder Krankheitsfall sind einige davon.

Ein weiterer wichtiger Aspekt ist die Tatsache, dass ein einzelner Administrator sich versehentlich aus dem Aareal Portal aussperren kann, beispielsweise indem er sein Passwort vergisst oder aber sich mehrfach bei der Eingabe vertippt. Selbstverständlich hilft Ihnen in einem solchen Fall Ihr Kundenberater der Aareal Bank gerne weiter und setzt Ihnen Ihr Passwort zurück.
Durch das Anlegen eines zweiten Benutzers mit Administrationsrechten sind Sie jedoch

auch in einer solchen Situation weiterhin handlungsfähig, unabhängig und schneller in der Lage, Ihren Benutzerzugang wieder freizuschalten.

Ihr Kundenberater wird für Sie gerne weitere Benutzer mit Administrationsrechten anlegen, bitte sprechen Sie ihn hierzu an!

5.4. Einem Benutzer neue Zugangsdaten vergeben

Es gibt verschiedene Situationen, die es erfordern, einem Benutzer neue Zugangsdaten zu vergeben:

- Sie haben entsprechend Kapitel 5.1 einen neuen Benutzer angelegt und möchten ihm die initialen Zugangsdaten zukommen lassen.
- Sie möchten einen gesperrten Benutzer wieder freigeben.
- Ein Benutzer hat sein Passwort vergessen oder dreimal ein falsches Passwort eingegeben. Sie wollen ihm nun ein neues (initiales) Passwort zuschicken.

Als Administrator werden Sie zu keinem Zeitpunkt das Passwort eines Benutzers einsehen oder ändern können. Durch dieses Sicherheitsmerkmal ist garantiert, dass Aktionen, die im Aktivitätenprotokoll zu einem Benutzer (siehe Kapitel 10) geführt werden, auch sicher diesem zugeordnet werden können. Schließlich kennt zu jedem Zeitpunkt nur er selbst das Passwort zu seinem Zugang.

Mit der Schaltfläche **ZUGANGSDATEN ANFORDERN** in der Benutzerverwaltung erstellen Sie ein neues initiales Passwort für den Benutzer, das Ihnen in Form eines PDF zum Herunterladen angeboten wird. Bitte lassen Sie dieses Dokument dem Benutzer zukommen.
Ein eventuell vorhandenes, bisheriges Passwort des Benutzers ist mit dem Anfordern neuer Zugangsdaten ungültig geworden.

Mit den im Schreiben enthaltenen Informationen kann sich der Benutzer erstmalig oder erneut am Aareal Portal anmelden. Er wird noch während des Anmeldeprozesses aufgefordert, ein eigenes Passwort zu wählen. Sobald er dies erledigt hat, erscheint er im Status „Zugangsdaten sind versendet/erstellt“.

Beim Durchlaufen des erstmaligen Anmeldungsprozesses wird gleichzeitig der imageTAN-Reader aktiviert. Dies geschieht durch das Scannen von Initialisierungsgrafiken und ist im Detail im Benutzerhandbuch in Kapitel 3 beschrieben.

Falls ein Benutzer sein Passwort vergessen hat und deshalb neue Zugangsdaten erhält, so bleibt der imageTAN-Reader aktiviert. Ebenso bleiben alle Schlüssel für die dem Benutzer zugeordneten EBICS-Teilnehmer-IDs erhalten und müssen nicht neu erzeugt werden.

5.5. Ein Schlüsselmedium durch den Administrator freischalten

Falls Sie dies möchten, können Sie festlegen, dass Schlüsselmedien durch Sie als Administrator manuell freigegeben werden müssen. Durch diese Maßnahme haben Sie als Administrator eine höhere Kontrolle über den Zeitpunkt, zu dem Sie einen Benutzer freischalten und eine generell höhere Sicherheit bei der Aktivierung neuer Benutzer.

! **Hinweis**: *Das Schlüsselmedium für einen Administratorzugang unterliegt immer der Freigabepflicht. Die Freigabe muss hierbei durch die Aareal Bank erfolgen.*

Um das Schlüsselmedium freigabepflichtig anzulegen, öffnen Sie den Dialog zum Anlegen eines neuen Benutzers oder zum Bearbeiten eines bereits vorhandenen Benutzers, wie in Kapitel 5.1 beschrieben. Öffnen Sie dann den zweiten Reiter **SCHLÜSSELMEDIUM** und setzen Sie den Haken bei **Schlüsselmedium freigabepflichtig**.
Bitte vergessen Sie nicht die Änderungen zu **ÜBERNEHMEN** und anschließend auf der Seite der Benutzerverwaltung zu **SPEICHERN**!

Der Benutzer erhält nun nach der Aktivierung seines imageTAN-Readers ein „Dokument zur imageTAN-Freischaltung“ zum Herunterladen angeboten, das er an Sie weiterleiten muss. Im Benutzerhandbuch ist dieser Schritt in Kapitel 3, Abbildung 6 dargestellt.

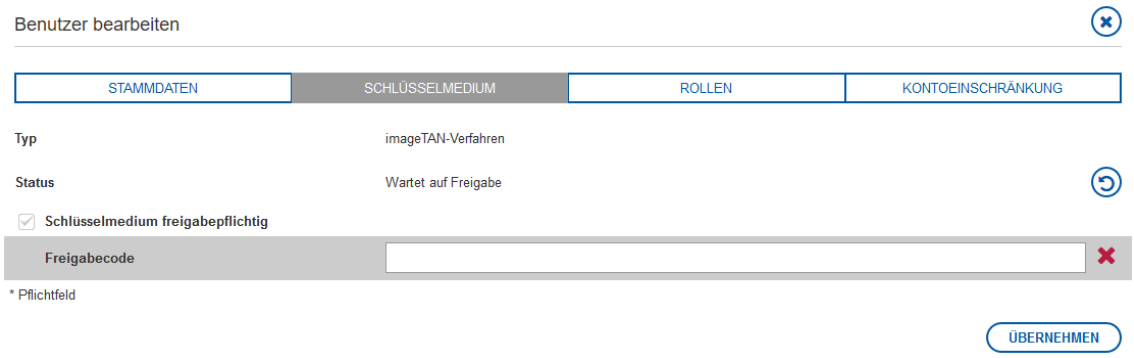

Abbildung 10: Freigabe eines Schlüsselmediums mit Hilfe des Freigabecodes

Tragen Sie den Freigabecode, den Sie mit dem Freischaltungsbrief vom Benutzer erhalten haben, im Reiter **SCHLÜSSELMEDIUM** der Maske Benutzer bearbeiten ein. Sobald der Code akzeptiert wurde, erscheint rechts neben dem Eingabefeld ein grüner Haken. Bestätigen Sie die Änderung mit **ÜBERNEHMEN** und **SPEICHERN** Sie wiederum die Änderungen in der Benutzerverwaltung.

Der Benutzer ist nun freigeschaltet.

Sollte der Benutzer vergessen haben, das Dokument herunterzuladen oder falls das Dokument verloren gegangen ist, klicken Sie bitte auf **ZUGANGSDATEN ANFORDERN** und lassen Sie den Benutzer den Prozess zur Erstanmeldung erneut durchlaufen.

5.6. Ihr eigenes Passwort ändern

Sie können jederzeit Ihr aktuelles Passwort ändern, das Sie zum Login ins Aareal Portal verwenden. Diese Möglichkeit steht jedem Benutzer des Aareal Portals zur Verfügung.

Öffnen Sie das Modul Administration und anschließend den Menüpunkt Profil. Sie gelangen automatisch zum Dialog zur Passwortänderung:

ADMINISTRATION ▶ PROFIL ▶ PASSWORTÄNDERUNG

Bitte geben Sie im nachfolgenden Dialog Ihr bisheriges Passwort und anschließend ein neues Passwort ein. Ein Indikator vermittelt Ihnen ein Gefühl für die Komplexität und damit für die Sicherheit des neuen Passworts.

> ***Hinweis**: Bitte wählen Sie zur Erhöhung Ihrer Sicherheit ein Passwort, das Sie ausschließlich für das Portal der Aareal Bank verwenden.*

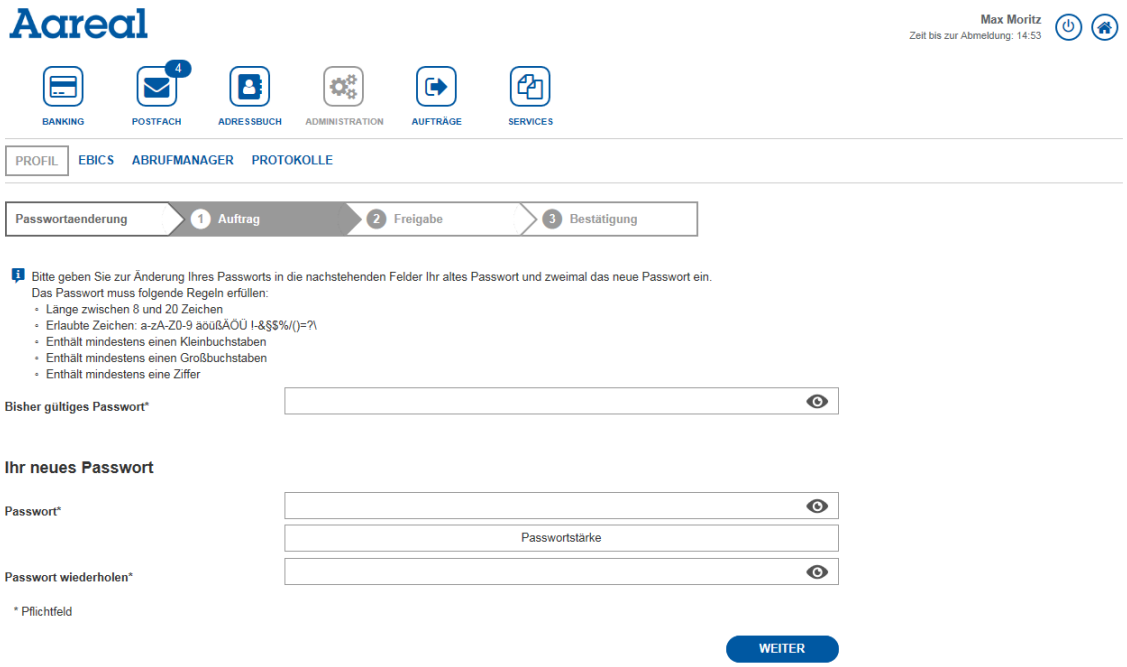

Abbildung 11: Änderung des eigenen Benutzerpasswords

Sollten Sie Ihr bisheriges Passwort zu ihrem Administratorzugang vergessen haben, wenden Sie sich bitte an Ihren Kundenberater der Aareal Bank. Er wird sich bemühen, Ihnen schnellstmöglich neue initiale Anmeldedaten zukommen zu lassen.

6. Rollen und Rechte

Nicht jeder Benutzer soll alle Funktionen des Aareal Portals nutzen und auf alle Daten Ihrer Konten zugreifen können. Hierfür bietet Ihnen das Aareal Portal zwei Möglichkeiten, um die Sicht auf Inhalte zu beschränken:

Mit Hilfe von Rollen fassen Sie Seiten des Aareal Portals zusammen, die Mitarbeiter bei der Ausführung typischer Tätigkeiten benötigen. So könnten Sie beispielsweise einem für die Buchhaltung zuständigen Mitarbeiter den Zugriff auf den Finanzstatus und das Postfach erteilen, jedoch nicht auf die Durchführung von Zahlungen. Ein anderer Mitarbeiter könnte Überweisungen und Lastschriften beauftragen, jedoch keine Berechtigung für die Beauftragung von Auslandszahlungen erhalten.

Da die Aufgaben in Ihrem Unternehmen individuell sind, können Sie Rollen definieren, die auf Ihre Bedürfnisse zugeschnitten sind. Jede Rolle können Sie anschließend einem oder mehreren Benutzern zuweisen. Wenn Sie einem Benutzer mehr als eine Rolle vergeben, addieren sich die darin enthaltenen Rechte.

Haben Sie mehrere Konten im Aareal Portal eingerichtet und möchten nicht jedem Benutzer Zugang zu allen Konten einräumen, so können Sie die Sicht mittels Kontoeinschränkungen verringern. Auch hier legen Sie portalweite Einschränkungen fest, die Sie dann einzelnen Benutzern zuweisen können.

Wie Sie Rollen und Kontoeinschränkungen Benutzern zuweisen, entnehmen Sie bitte Kapitel 5.1 weiter oben im Handbuch. Die folgenden Kapitel beschreiben deren Anlage und Verwaltung.

6.1. Rollen anlegen und verwalten

Öffnen Sie das Modul Administration und anschließend den Menüpunkt Rollen und Rechte:

ADMINISTRATION ▶ ROLLEN UND RECHTE ▶ ROLLENDEFINITION

Sie sehen daraufhin eine Liste aller für Sie zur Verfügung stehenden Rollen. Auch wenn Sie noch keine eigenen Rollen definiert haben, steht Ihnen mindestens die folgende Rollendefinition bereits zur Verfügung:

- **Kontoeinsicht für Dritte** ermöglicht einem Benutzer, lesend auf die im Portal vorhandenen Kontoumsätze Einsicht zu nehmen.

Darüber hinaus hat Ihr Administrator der Aareal Bank möglicherweise Rollen angelegt, die Sie nutzen können. Mehr dazu erfahren Sie weiter unten im Kapitel.

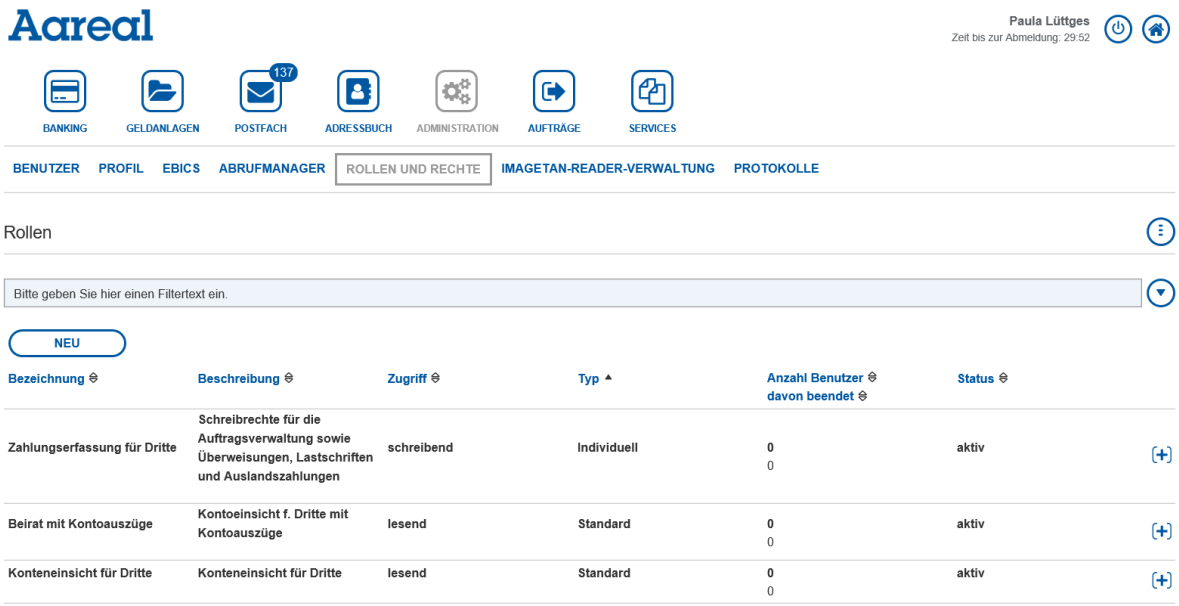

Abbildung 12: Übersicht über vorhandene Rollen

Um eine neue Rolle anzulegen, benutzen Sie bitte die Schaltfläche **NEU** oben links. Es öffnet sich der in Abbildung 13 ausschnittsweise gezeigte Dialog.

Vergeben Sie zunächst eine **Bezeichnung** und anschließend eine **Beschreibung**, die den Zweck der Rolle für Sie und andere Administratoren erkennbar wiedergibt.

Darunter sehen Sie eine Möglichkeit zur Einschränkung **Nur Leseberechtigung**. Mit dem Setzen des Hakens kann der Benutzer, dem diese Rolle zugeordnet wird, auf die im Folgenden ausgewählten Seiten nur lesend zugreifen.

Sollten Sie eine Rolle mit gemischten Rechten, lesend und schreibend, vergeben wollen, so legen Sie bitte zwei Rollen an und weisen Sie dem Benutzer beide Rollen zu. Alle einem Benutzer zugewiesenen Rollen addieren sich. Dabei überlagert immer die höherwertige Berechtigung die niedrigere:
Erhält ein Benutzer beispielsweise durch eine Rolle ein lesendes Recht auf die Unterschriftenmappe, durch eine zweite ein schreibendes, so kann er auf die Unterschriftenmappe schreibend zugreifen.

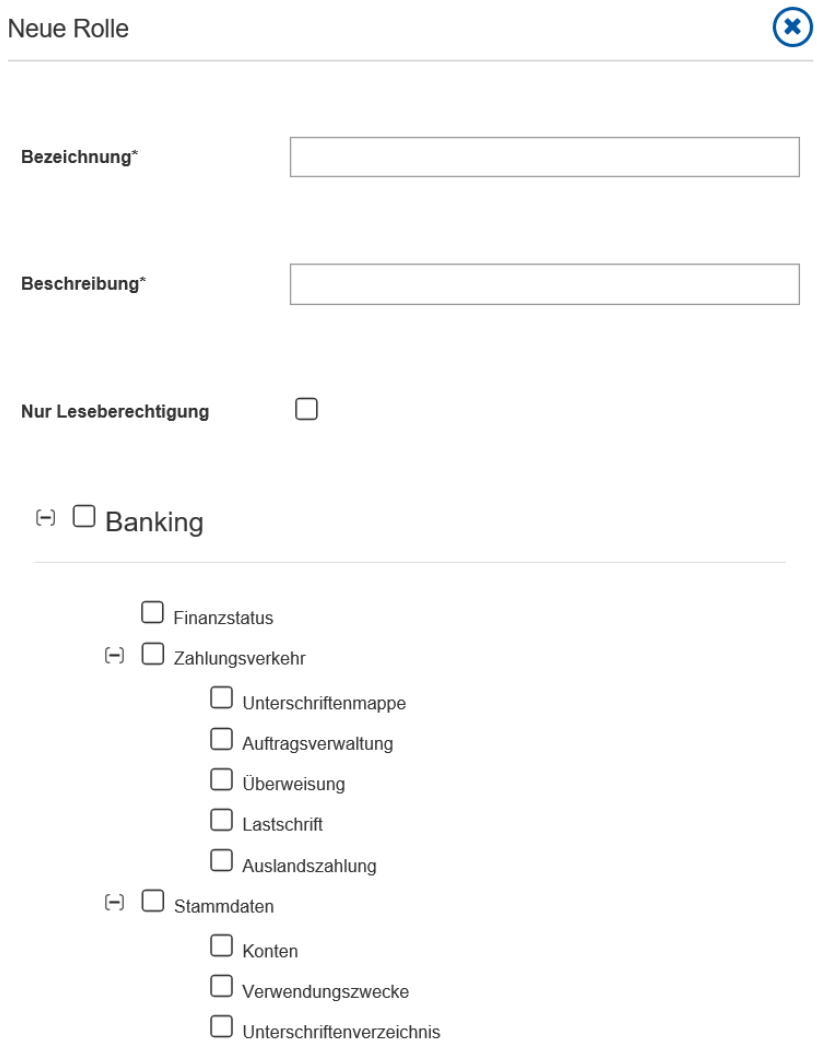

Abbildung 13: Ein Ausschnitt des Dialogs zum Anlegen einer neuen Rolle

Selektieren Sie nun diejenigen Seiten des Aareal Portals, die dem Inhaber der Rolle freigegeben werden sollen. Im Bereich des Postfachs können Sie auch individuell angelegte Verzeichnisse freigeben. Es bietet sich an, diese Verzeichnisse vor der Definition von Rollen anzulegen. Andernfalls denken Sie bitte daran, die neu angelegten Verzeichnisse nachfolgend in die Definition der entsprechenden Rollen aufzunehmen.

Speichern Sie die neue Rolle mit der Schaltfläche SPEICHERN unten rechts.

Die neu angelegte Rolle ist nun in der Tabelle **Rollen** aufgelistet.

In der Spalte Zugriff sehen Sie, ob die Rolle **lesende** oder **schreibende** Rechte vergibt.

Am **Typ** erkennen Sie, ob Sie die Rolle selbst angelegt haben („Individuell“), oder ob diese durch den Administrator der Aareal Bank („Standard“) für Sie hinterlegt wurde. Bitte beachten Sie, dass Sie nur selbst angelegte Rollen ändern und löschen können.

Anzahl Benutzer zeigt Ihnen an, wie viele Benutzer die jeweilige Rolle verwenden. Diese Information ist wichtig, um abschätzen zu können, ob Sie eine Rollendefinition im laufenden Betrieb ändern können.

In der Zeile darunter erfahren Sie, wie viele der oben gezeigten Benutzer **davon beendet** und damit dauerhaft nicht mehr aktiv sind.

Unter **Status** sehen Sie, ob die Rolle noch aktiv oder beendet ist. Sie können individuelle Rollen löschen, indem Sie auf das **[+]** des entsprechenden Eintrags klicken und dann auf die Schaltfläche **LÖSCHEN**.

Gelöschte Rollendefinitionen können nicht wieder aktiviert werden. Sie bleiben im Aareal Portal im Status „Beendet“ gespeichert, um die Nachvollziehbarkeit zu einem späteren Zeitpunkt zu gewährleisten. Somit kann die exakte Bezeichnung auch nicht erneut vergeben werden.

Standardmäßig werden gelöschte Rollendefinitionen ausgeblendet. Um sie anzuzeigen, wählen Sie rechts neben dem Eingabefeld für die Schnellfilterung den Eintrag **ERWEITERTE SUCHE** und wählen Sie im Feld **Status** den Wert beendet aus. Nach der Bestätigung mit der Schaltfläche **SUCHEN** sehen Sie alle gelöschten Rollen.

6.2. Kontoeinschränkungen anlegen und verwalten

Mit Hilfe von Kontoeinschränkungen können Sie festlegen, welche Benutzer Einblick auf welche Konten erhalten. Das Vorgehen ist vergleichbar mit der Anlage von Rollen: Als Administrator legen Sie Vorlagen für Kontoeinschränkungen fest und weisen diese anschließend einem oder mehreren Benutzern zu. Alternativ können Sie auch im Bearbeitungsdialog eines einzelnen Benutzers im letzten Reiter Kontoeinschränkungen vornehmen. Diese gelten dann nur für diesen einen Benutzer.

Sollten Sie mit Konten von anderen Banken als der Aareal Bank im Aareal Portal arbeiten wollen, so richten Sie diese bitte ein, bevor Sie Kontoeinschränkungen hinterlegen.

Öffnen Sie das Modul Administration und anschließend den Menüpunkt Rollen und Rechte:

ADMINISTRATION ▶ ROLLEN UND RECHTE ▶ KONTOEINSCHRÄNKUNG

Sie sehen daraufhin eine Liste aller für Sie zur Verfügung stehenden Kontoeinschränkungen. Wenn Sie das Aareal Portal zum ersten Mal betreten, wird die Liste leer sein:

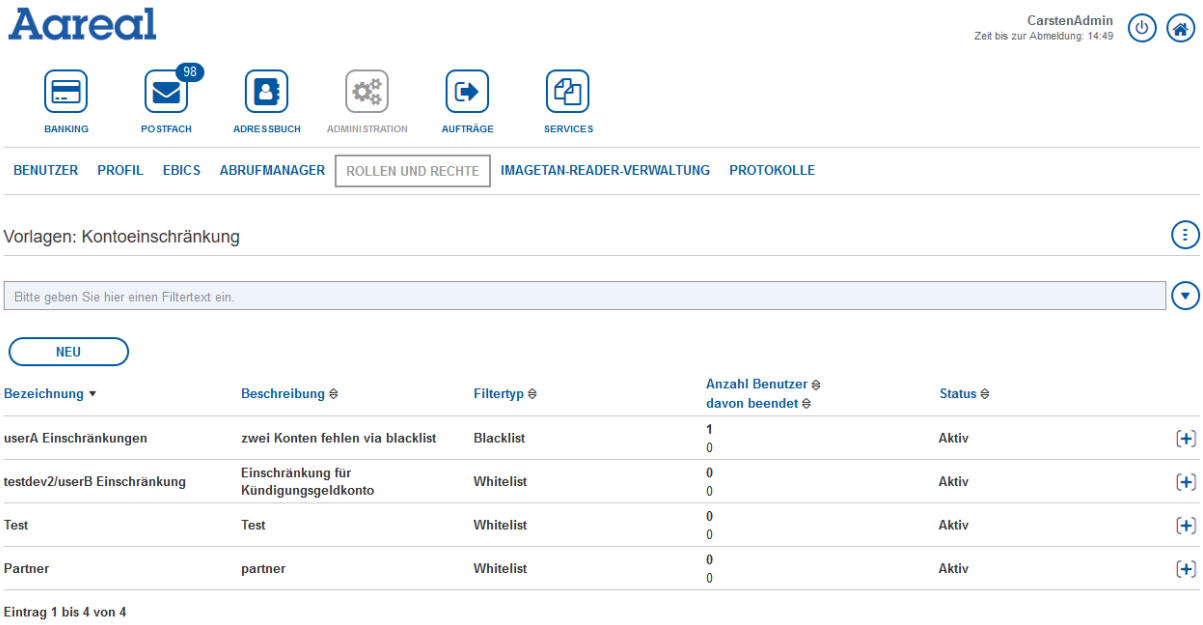

Abbildung 14: Übersicht Ihrer Vorlagen für Kontoeinschränkungen

Um eine neue Vorlage für eine Kontoeinschränkung anzulegen, drücken Sie auf die Schaltfläche **NEU** oben links. Es öffnet sich der in Abbildung 15 gezeigte Dialog.

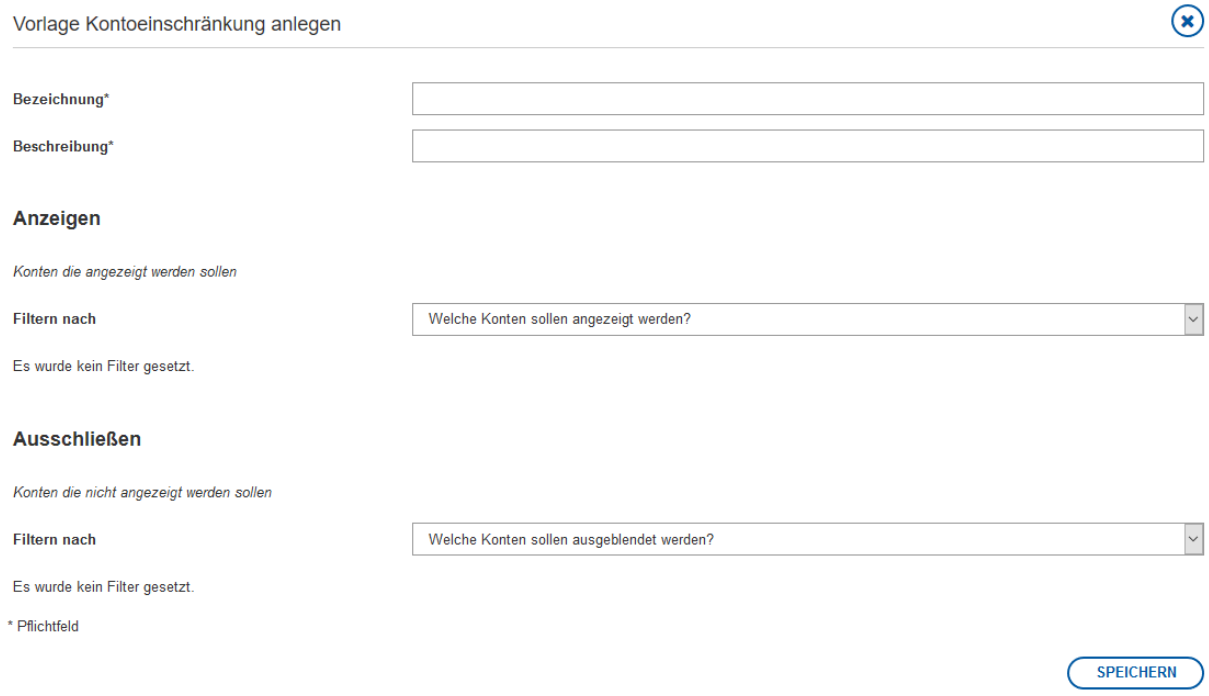

Abbildung 15: Dialog zur Anlage einer neuen Kontoeinschränkung

Vergeben Sie zunächst eine eindeutige **Bezeichnung** und anschließend eine **Beschreibung**, die den Zweck der Kontoeinschränkung für Sie und andere Administratoren erläutert. Anhand dieser beiden Werte werden Sie die Kontoeinschränkung später wiedererkennen und nachvollziehen können.

Solange im Aareal Portal keine Kontoeinschränkungen angelegt und Benutzern zugewiesen sind, kann ein Benutzer alle im Aareal Portal angelegten Konten einsehen. Um Einschränkungen zu beschreiben, stehen Ihnen zwei Möglichkeiten zur Verfügung:

- Sie können auf positive Art festlegen, welche Konten explizit erlaubt sind. Sobald einem Benutzer mindestens eine dieser als Whitelist bezeichneten Kontoeinschränkungen zugewiesen wurde, werden alle Konten ausgeblendet, die nicht von einer dieser Whitelistdefinitionen erfasst werden.

  Beispielsweise können Sie eine Einschränkung hinterlegen, die dem Benutzer Zugriff auf alle Konten mit der Bezeichnung „Kündigungsgeldkonto“ erlaubt. Alle von dieser (und ggf. weiterer dem Benutzer zugewiesenen) Einschränkung nicht erfassten Konten würden ausgeblendet.

- Alternativ können Sie auf negative Art Konten ausdrücklich von der Anzeige ausnehmen. Diese als Blacklist bezeichneten Einschränkungen zeigen dem Benutzer alle Konten an, die nicht von dieser erfasst werden.

Darüber hinaus haben Sie auch die Möglichkeit, diese beiden Erfassungsarten zu kombinieren. Beispielsweise könnten Sie eine Einschränkung anlegen, die dem Benutzer ausschließlich Zugriff auf Konten der Art „Kündigungsgeldkonto“ erlaubt, mit Ausnahme des oder der Konten, die Sie explizit angegeben haben.

Natürlich können Sie Kontoeinschränkungen auch separat anlegen und miteinander kombinieren, indem Sie sie einem Benutzer zuweisen.

Erfassen Sie eine positive Einschränkung mit Hilfe der Eingabefelder im Bereich **Anzeigen**:

Wählen Sie in der Auswahlliste **Filtern nach** eines der Selektionskriterien aus:

- Kontonummer (IBAN)
- Kontosystem-ID
- Banken (BIC)
- Kontoinhaber
- Treugeber
- Kontobezeichnung

Im darunterliegenden Eingabefeld **Filter** geben Sie nun den Wert an, nach dem gefiltert werden soll und betätigen Sie die mit einem **+** gekennzeichnete Schaltfläche rechts. Sie können auf diese Weise weitere Filter eingeben und hinzufügen, die Werte erscheinen unterhalb in der Liste.

! ***Hinweis***: *Innerhalb einer Einschränkung können Sie immer nur ein Filterkriterium eingeben.*

Sollten Sie Werte wieder entfernen wollen, markieren Sie die entsprechenden Einträge und klicken Sie auf **MARKIERTE EINTRÄGE LÖSCHEN** oder setzen Sie den gesamten Filter zurück, indem Sie auf **FILTER ZURÜCKSETZEN** klicken.

Um eine negative Einschränkung zu erfassen, benutzen Sie die Eingabefelder im Bereich **Ausschließen**:

Die Auswahlliste **Filtern nach** bietet Ihnen gegenwärtig nur die Möglichkeit, einzelne Kontonummern gezielt auszublenden. Geben Sie eine oder mehrere IBANs ein, wie im Bereich **Anzeigen** beschrieben.

Wenn Sie alle Werte erfasst haben, SPEICHERN Sie Ihre Eingaben.

Die neu angelegte Kontoeinschränkung ist nun in der in Abbildung 14 gezeigten Tabelle **Vorlagen: Kontoeinschränkung** aufgelistet.

Je nachdem, ob Sie Werte im Bereich Anzeigen oder im Bereich Ausblenden erfasst haben, wird Ihre neue Kontoeinschränkung in der Spalte **Filtertyp** als **Whitelist** oder **Blacklist** angezeigt. Falls Sie in beiden Bereichen Kriterien hinterlegt haben, erscheint die Einschränkung als Filtertyp **kombiniert**.

Anzahl Benutzer zeigt Ihnen an, wie viele Benutzer die jeweilige Kontoeinschränkung verwenden. Diese Information ist wichtig, um abschätzen zu können, ob Sie eine Kontoeinschränkung im laufenden Betrieb ändern können.
In der Zeile darunter erfahren Sie, wie viele der oben gezeigten Benutzer **davon beendet** und damit gelöscht und archiviert wurden.

Unter **Status** sehen Sie, ob die Kontoeinschränkung noch aktiv oder beendet ist. Sie können individuelle Einschränkungen löschen, indem Sie auf das **[+]** des entsprechenden Eintrags klicken und dann auf die Schaltfläche LÖSCHEN.

Gelöschte Kontoeinschränkungen können nicht wieder aktiviert werden. Sie bleiben im Aareal Portal im Status „Beendet“ gespeichert, um die Nachvollziehbarkeit zu einem späteren Zeitpunkt zu gewährleisten. Somit kann die exakte Bezeichnung auch nicht erneut vergeben werden.

Standardmäßig werden beendete Kontoeinschränkungen ausgeblendet. Um sie anzuzeigen, wählen Sie rechts neben dem Eingabefeld für die Schnellfilterung den Eintrag ERWEITERTE SUCHE und wählen Sie im Feld **Status** den Wert beendet aus. Nach der Bestätigung mit der Schaltfläche SUCHEN sehen Sie alle beendeten Kontoeinschränkungen.

7. Verwaltung der imageTAN-Reader

Um Ihnen ein Höchstmaß an Sicherheit bieten zu können, verlangt das Aareal Portal bei der Anmeldung zusätzlich zu Ihrem persönlichen Passwort, sowie bei finanziellen Aufträgen an die Bank die Eingabe einer jedes Mal neu generierten TAN. Über diese TAN weisen Sie als Benutzer nach, dass Sie zusätzlich zu ihrem gültigen Passwort auch im Besitz des auf Sie registrierten Schlüsselmediums sind.

Der imageTAN-Reader generiert die benötigten TANs für Sie. Hierzu scannen Sie eine auf dem Bildschirm gezeigte Grafik ab und geben die daraufhin vom imageTAN-Reader angezeigte TAN im Aareal Portal ein. Der imageTAN-Reader ist dabei an Ihren spezifischen Zugang gebunden und kann nur für diesen TANs generieren. Somit ist ein Missbrauch durch Dritte ausgeschlossen.

Dieses Kapitel beschreibt alle Funktionen im Aareal Portal und am imageTAN-Reader, die Sie für Ihre Arbeit als Administrator benötigen.

7.1. Aktivierte imageTAN-Lizenzen einsehen und freigeben

Um einen Überblick über alle derzeit aktivierten und von Benutzern verwendeten Lizenzen – und damit über die sich im Einsatz befindlichen imageTAN-Reader – zu erhalten, öffnen Sie im Modul Administration diese Seite:

ADMINISTRATION ▶ IMAGETAN-READER-VERWALTUNG

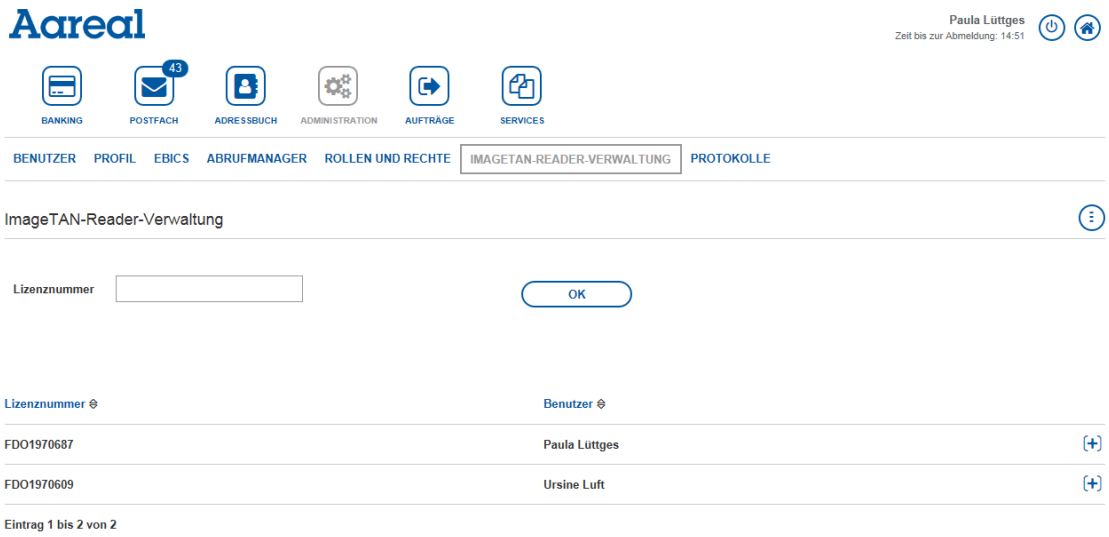

Abbildung 16: Übersicht über alle aktivierten imageTAN-Reader

Die Tabelle listet Ihnen alle **Lizenznummern** auf, die von den imageTAN-Readern der jeweiligen **Benutzer** aktiv genutzt werden.

Sie können eine Lizenz gezielt suchen, indem Sie die Lizenznummer am oberen Ende der Seite eingeben und auf die Schaltfläche **OK** drücken.

Sollte ein Benutzer seinen imageTAN-Reader verloren haben, können Sie diesen deaktivieren, indem Sie ihm die Lizenz entziehen. Klicken Sie in der Zeile des

entsprechenden Benutzers auf das **[+]** und dann auf die Schaltfläche **IMAGETAN-READER ZURÜCKSETZEN**. Bestätigen Sie dann die anschließende Sicherheitsabfrage.

Mit dem Zurücksetzen des Readers werden alle EBICS-Schlüssel zu diesem Benutzer gelöscht. Ebenso wird die PIN des Benutzers gelöscht. Der imageTAN-Reader kann nun wieder einem neuen Benutzer zugewiesen werden.

Wie Sie aus einem gefundenen oder zurückerhaltenen Gerät die Lizenznummer auslesen, erfahren Sie im nachfolgenden Kapitel 7.2.

7.2. Einstellungen am imageTAN-Reader vornehmen

Jeder imageTAN-Reader verfügt über ein Menü für die Konfiguration. Sie erreichen dieses Menü, indem Sie in ausgeschaltetem Zustand den Ein-/Aus-Knopf am oberen Ende des Gerätes mindestens 3 Sekunden gedrückt halten:

Abbildung 17: Einstellungen am imageTAN-Reader

Sie sehen ein **Einstellungen**-Menü mit den in Abbildung 17 gezeigten Einträgen:

- Wählen Sie im Menüpunkt **Sprache** eine für den Benutzer geeignete Sprache aus.

- Unter **Aktivierungen** sehen Sie die aktuell genutzte Lizenznummer, sofern das Gerät aktiviert ist. Falls Sie ein Gerät finden oder einem Benutzer nicht eindeutig zuordnen können, so können Sie über die Lizenznummer im Menü **ADMINISTRATION ▶ IMAGETAN-READER-VERWALTUNG** den zugehörigen Benutzer herausfinden und gegebenenfalls die Lizenz deaktivieren. Lesen Sie Kapitel 7.1 für weitere Informationen.

- Über den Eintrag **Aktivierung löschen** kann die aktive Lizenznummer vom Gerät entfernt werden. Diese Funktion ist durch Abfrage der Geräte-PIN zusätzlich abgesichert. Das Gerät kann anschließend nicht mehr für die Anmeldung am Aareal Portal oder für Zahlungen verwendet werden.

  ! **Hinweis**: *Bitte beachten Sie, dass die Lizenznummer im Aareal Portal auch weiterhin dem Benutzer zugeordnet ist. Sie wurde lediglich am imageTAN-Reader deaktiviert. Setzen Sie den imageTAN-Reader am Benutzer zurück, wie in Kapitel 7.1 beschrieben.*

  Benutzen Sie diese Funktion beispielsweise, falls der imageTAN-Reader noch auf einen vorherigen, bereits deaktivierten Benutzer registriert ist.
  Die primäre Methode, einen imageTAN-Reader zu deaktivieren, ist die oben beschriebene Nutzung der imageTAN-Reader-Verwaltung. Möglich ist aber auch die Verwendung des Links „ImageTAN-Reader sperren?“ (siehe Abbildung 18) auf der Anmeldemaske durch den Benutzer selbst. Als Administrator verwenden Sie in diesem Fall bitte den Link zum Widerruf des Schlüsselmediums auf dem Reiter **SCHLÜSSELMEDIUM** im Dialog zum Bearbeiten des Benutzers (siehe Abbildung 6).

- Über **PIN ändern** kann der Benutzer seine selbstgewählte PIN am imageTAN-Reader jederzeit ändern. Wie Sie eine neue PIN setzen, falls Sie Ihre aktuelle PIN nicht mehr kennen, erfahren Sie in Kapitel 7.3.1 und Kapitel 7.3.2.

- Mit **PIN entsperren** können Sie eine neue PIN vergeben, sollten Sie sich an ihre bisherige PIN nicht mehr erinnern können und das Gerät durch mehrfache Falscheingabe gesperrt haben.

- Der letzte Eintrag **Manuelle Eingabe** ist derzeit noch ohne Funktion und wird gegebenenfalls zukünftig verwendet.

7.3. Fehlerzustände beheben

7.3.1. Der Benutzer hat seine PIN vergessen

Ein Benutzer, der seine PIN unwiderruflich vergessen hat, kann sich über den Link „PIN vergessen oder gesperrt“ in der Anmeldemaske (siehe Abbildung 18) eine neue PIN vergeben. Die genaue Vorgehensweise ist im nachfolgenden Kapitel 7.3.2 beschrieben.

Um zu dieser Eingabemaske zu gelangen, muss er sein Passwort kennen. Sollte er - beispielsweise auf Grund längerer Inaktivität - auch dieses vergessen haben, fordern Sie für den Benutzer neue Zugangsdaten an, wie in Kapitel 5.4 beschrieben.

Eine weitere Möglichkeit für Sie als Administrator ist es, den imageTAN-Reader des Benutzers im Portal zurückzusetzen. Benutzen Sie hierfür die Schaltfläche **IMAGETAN-READER ZURÜCKSETZEN** in der **IMAGETAN-READER-VERWALTUNG**. Details hierzu finden Sie in Kapitel 7.1.

! **Hinweis**: *Bei der Sperrung des imageTAN-Readers werden auch alle EBICS-Schlüssel zurückgesetzt. Diese müssen entsprechend Kapitel 6.2.3 des Benutzerhandbuchs im Anschluss neu erzeugt werden.*

7.3.2. Der Benutzer hat sein Gerät durch Falscheingabe der PIN gesperrt

Ein Benutzer kann TANs mit dem imageTAN-Reader nur erzeugen, nachdem er seine PIN eingegeben hat. Diese hat er während der Aktivierung des imageTAN-Readers selbst gewählt.

Zur Eingabe der korrekten PIN stehen ihm insgesamt drei Versuche zur Verfügung. Hat er bei der insgesamt dritten Eingabe – auch zeitliche Unterbrechungen oder ein Neustart des imageTAN-Readers starten diesen Zähler nicht neu – noch nicht die richtige PIN eingegeben, so wird die PIN gesperrt. Der Reader zeigt die Meldung „Ihre PIN wurde gesperrt. Bitte wenden Sie sich an Ihren Administrator.“ Darunter wird ein sechsstelliger Entsperrcode angezeigt.

Der Benutzer kann das Gerät selbständig wieder entsperren und sich eine neue PIN vergeben. Hierzu meldet er sich wie gewohnt am Aareal Portal mit seinen Logindaten an.

Am unteren Ende der Seite für den Login findet er einen Link „PIN vergessen oder gesperrt?“.

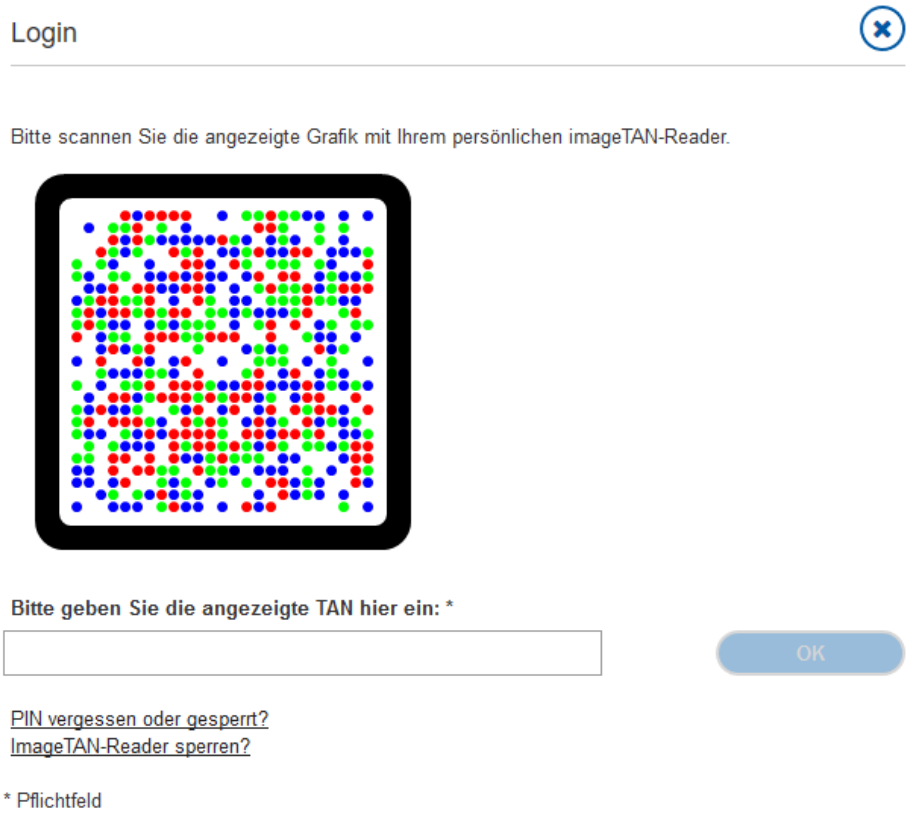

Abbildung 18: Die Seite für den Login

Nach einem Klick auf diesen Link wird der Benutzer aufgefordert, den sechsstelligen Entsperrcode einzugeben.

Der Benutzer muss nun am imageTAN-Reader das Einstellungen-Menü öffnen, wie in Kapitel 7.2 beschrieben. Anschließend muss er den Eintrag **PIN entsperren** wählen und den Entsperrcode im Dialog des Aareal Portals eingeben.

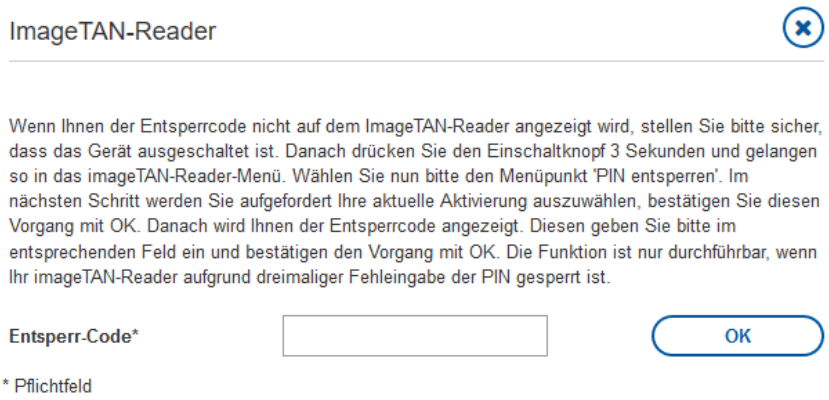

Abbildung 19: Entsperrung des imageTAN-Readers mit Hilfe des Entsperrcodes

Der Benutzer wird darauf hingewiesen, dass mit der Neuvergabe der PIN alle EBICS-Schlüssel verfallen und er sich bei allen Banken neu initialisieren muss. Dies ist mit **JA** zu bestätigen.

Der nächste Dialog zeigt den Freigabecode an, der am imageTAN-Reader einzugeben ist. Sollte dieser sich zwischenzeitlich ausgeschaltet haben, ist erneut das **Einstellungen**-Menü zu öffnen und **PIN entsperren** erneut auszuwählen.

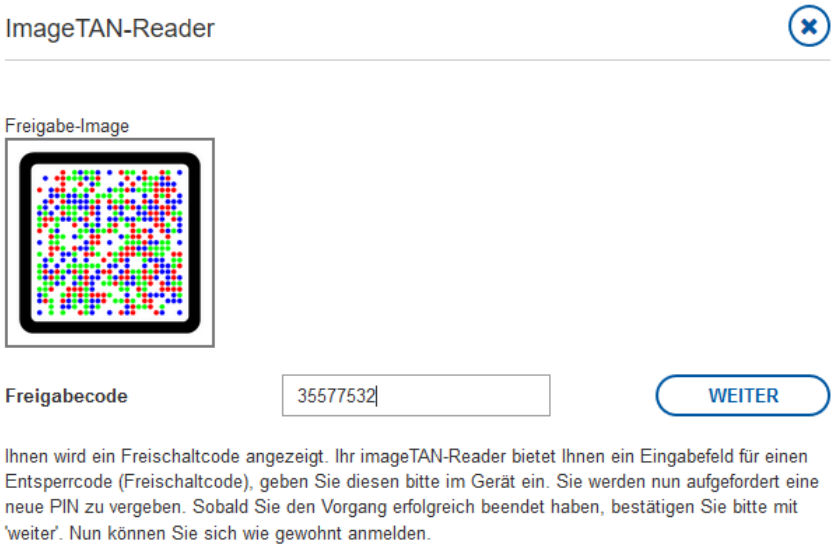

Abbildung 20: Der Freigabecode zur Vergabe einer neuen PIN

Anschließend ist eine neue PIN zu wählen und die Eingabe zu wiederholen. Der Benutzer kann sich nun erneut am Aareal Portal anmelden.

Bitte denken Sie daran, die EBICS-Schlüssel neu zu generieren, wie in Kapitel 6.2.3 im Benutzerhandbuch beschrieben.

7.3.3. Der Benutzer hat seinen imageTAN-Reader verloren

Sollte ein Benutzer feststellen, dass er seinen imageTAN-Reader verloren hat, so ist es wichtig, diesen so schnell wie möglich zu sperren. Das kann entweder der Benutzer selbst durchführen, oder Sie als Administrator übernehmen diese Aufgabe für ihn.

Ein Benutzer kann über den Link „ImageTAN-Reader sperren?“ auf der Anmeldemaske (siehe Abbildung 18) die Sperrung vornehmen. Um zu diesem Link zu gelangen, benötigt der Benutzer seine Anmeldedaten inkl. Passwort.

Sobald er auf diesen Link klickt, erscheint die in Abbildung 21 dargestellte Sicherheitsabfrage. Er wird darauf hingewiesen, dass der Benutzerzugang sofort gesperrt wird und auch alle EBICS-Schlüssel gelöscht werden.

Um den Benutzer wieder zu aktivieren, schicken Sie ihm einen neuen imageTAN-Reader zu und folgen Sie den Anweisungen aus Kapitel 5.4.

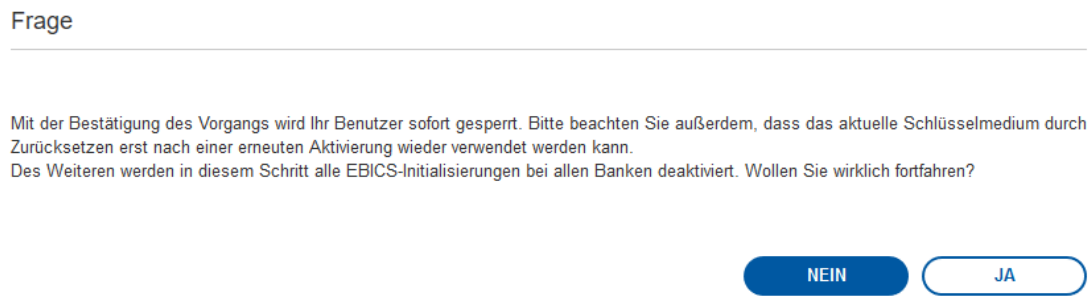

Abbildung 21: Sicherheitsabfrage vor dem Sperren des imageTAN-Readers

Alternativ können Sie als Administrator den imageTAN-Reader des entsprechenden Benutzers deaktivieren. Auch in diesem Schritt werden alle EBICS-Schlüssel gelöscht. Suchen Sie sich hierfür im Menü **ADMINISTRATION ▶ BENUTZER** den betroffenen Benutzer heraus, klicken Sie auf den Eintrag des Benutzers und wechseln Sie auf den Reiter **SCHLÜSSELMEDIUM**. Betätigen Sie nun die kleine Schaltfläche mit dem Pfeil entgegen des Uhrzeigersinns auf der rechten Seite.

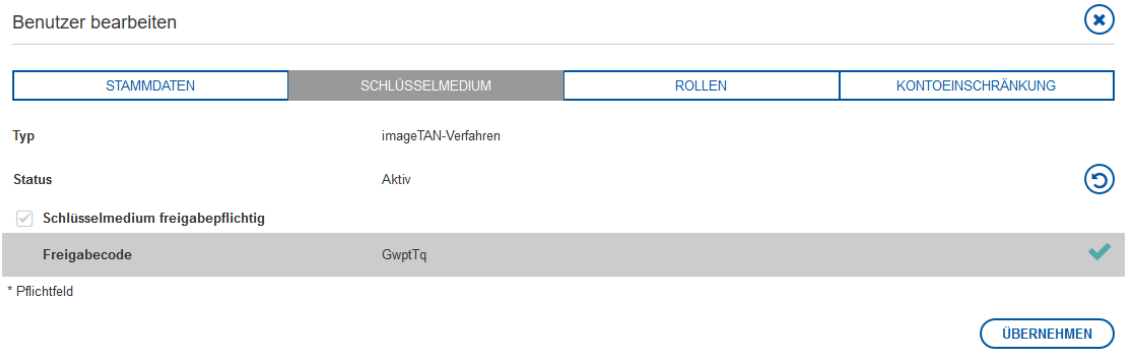

Abbildung 22: Invalidierung eines imageTAN-Readers im Reiter Schlüsselmedium

Der bisherige imageTAN-Reader des Benutzers wurde nun deaktiviert und kann nicht mehr zur Anmeldung am Aareal Portal genutzt werden. Der Benutzer kann sich mit einem neuen imageTAN-Reader am Aareal Portal anmelden, seine Kundenkennung, Benutzerkennung und sein Passwort sind weiterhin gültig. Bei der nächsten Anmeldung wird er aufgefordert, seinen imageTAN-Reader erneut zu aktivieren. Dieser Prozess verläuft analog dem Vorgehen bei der Erstanmeldung. Im Anschluss daran ist es notwendig, dass der Benutzer die EBICS-Schlüssel neu initialisiert.

Um das Schlüsselmedium eines Administrators zu deaktivieren, wenden Sie sich bitte an Ihren Kundenberater der Aareal Bank.

7.3.4. Ein verlorener imageTAN-Reader taucht wieder auf

Um herauszufinden, ob ein imageTAN-Reader einem Benutzer zugeordnet ist, lesen Sie zunächst die Lizenznummer aus dem Gerät aus. Die Vorgehensweise dazu ist in Kapitel 7.2 im Abschnitt **Aktivierungen** beschrieben.
Mit Hilfe der Lizenznummer aus dem imageTAN-Reader können Sie nun im Menü

ADMINISTRATION ▶ IMAGETAN-READER-VERWALTUNG nachsehen, welchem Benutzer das Gerät zugeordnet ist.

Ist das Gerät nicht aktiviert, d. h. im Abschnitt **Aktivierungen** des imageTAN-Readers ist kein Eintrag enthalten, so ist das Gerät keinem Benutzer zugeordnet. Das Gerät ist in seinem Grundzustand und einsatzbereit.

Können Sie das Gerät einem Benutzer zuordnen und möchte dieser Benutzer mit dem Gerät weiterarbeiten (z. B. weil er das Gerät verloren hat), dann geben Sie dem Benutzer das Gerät zurück. Sollte er seine PIN zwischenzeitlich aus Sicherheitsgründen gesperrt haben, so kann er ihn über den Link **PIN vergessen oder gesperrt?** (vgl. Abbildung 18) wieder entsperren.
Erinnern Sie ihn ggf. daran, dass er im Anschluss an die Entsperrung des Gerätes seine EBICS-Schlüssel neu initialisieren muss. Die Vorgehensweise hierzu ist in Kapitel 6.2.3 im Benutzerhandbuch erklärt.

Für den Fall, dass Sie ein aktiviertes Gerät zurückerhalten, für das Sie keinen Benutzer identifizieren können, oder falls der Benutzer mittlerweile mit einem Ersatzgerät arbeitet und Sie die Aktivierung löschen möchten, ohne die PIN des Gerätes zu kennen, schicken Sie den imageTAN-Reader bitte an die Aareal Bank zurück.

8. Benutzern EBICS-Teilnehmer zuordnen

Ein Benutzerzugang zum Aareal Portal ermöglicht es einem Benutzer, sich anzumelden und auf die im Aareal Portal gespeicherten Daten zuzugreifen. Damit ein Benutzer darüber hinaus Kontoumsätze der Aareal Bank oder einer anderen Bank abrufen und Aktivitäten wie das Freigeben von Zahlungsaufträgen durchführen kann, benötigt er eine entsprechende EBICS-Berechtigung der jeweiligen Bank. In diesem Kapitel erfahren Sie, wie Sie Benutzer mit EBICS-Berechtigungen ausstatten, und so die Berechtigung auf Konten verwalten.

Sollten Sie mit EBICS-Berechtigungen noch nicht vertraut sein, lesen Sie bitte Kapitel 5.2 im Benutzerhandbuch. Tabelle 1 gibt einen schnellen Überblick über die zur Verfügung stehenden Berechtigungen A, B, E und T.

Für die folgenden Schritte benötigen Sie vorkonfigurierte EBICS-Teilnehmer von allen im Aareal Portal eingerichteten Banken. Bitte sprechen Sie Ihren Kundenberater an, sollten Ihnen die EBICS-Teilnehmer nicht vorliegen.

Zudem müssen Sie die für die Durchführung der folgenden Schritte erforderlichen Bankparameter bereits konfiguriert haben. Kapitel 6.2.1 im Benutzerhandbuch erläutert Ihnen die Einzelheiten.

Um einen Benutzer mit einer einsatzbereiten EBICS-Berechtigung auszustatten, sind zwei Schritte notwendig:

- Zuerst wird dem Benutzer ein EBICS-Teilnehmer zugeordnet. Der EBICS-Teilnehmer definiert die Berechtigungen zum Zugriff auf die Konten bei einer Bank. Falls ein Benutzer auf Konten mehrerer Banken berechtigt werden soll, muss ihm für jede Bank ein EBICS-Teilnehmer zugewiesen werden.

  Diesen Schritt kann entweder ein Administrator für alle Benutzer durchführen, oder ein Benutzer kann sich selbst EBICS-Teilnehmer zuweisen.
  Wie sie die Zuordnung von EBICS-Teilnehmern für andere Benutzer übernehmen, erfahren Sie in diesem Kapitel weiter unten. Möchten Sie dagegen sich selbst einen EBICS-Teilnehmer zuordnen, lesen Sie bitte Kapitel 6.2.3 im Benutzerhandbuch.

- Im zweiten Schritt muss jeder neu zugewiesene EBICS-Teilnehmer initialisiert werden. Hierbei werden mit Hilfe des imageTAN-Readers Schlüssel erzeugt, die der Authentifizierung des Benutzers bei der jeweiligen Bank und für die Verschlüsselung der Kommunikation dienen. Diesen Schritt muss jeder Benutzer selbst erledigen. Die einzelnen Schritte sind ebenfalls im Benutzerhandbuch in Kapitel 6.2.3 beschrieben.

Öffnen Sie im Modul Administration die Seite zur Konfiguration der Bankparameter:

ADMINISTRATION ▶ EBICS ▶ BANKPARAMETER

Klicken Sie dann auf das **[+]**-Symbol des entsprechenden Bankparameters, für den Sie EBICS-Berechtigungen vergeben möchten, und klicken Sie auf **ÄNDERN**. Es öffnet sich der Dialog **Bankparameter Detailansicht**. Öffnen Sie nun den letzten Reiter **Teilnehmer**:

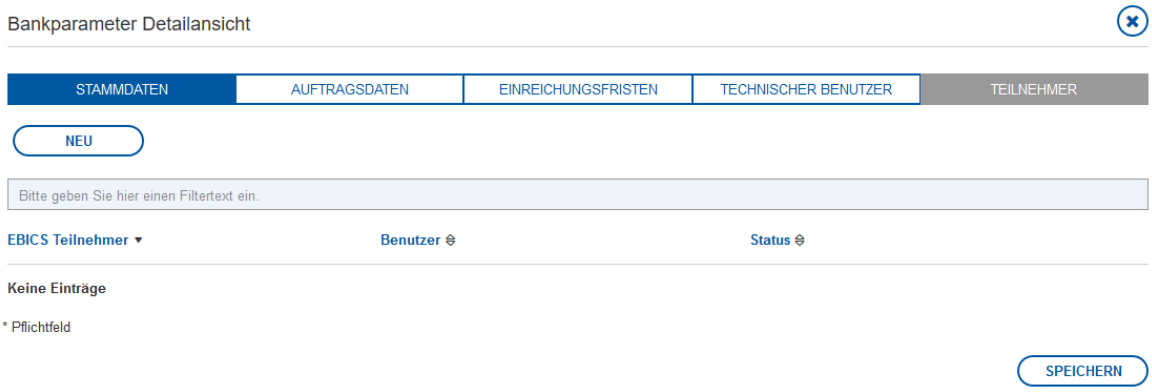

Abbildung 23: Zuordnung von EBICS-Teilnehmern zu Benutzern

Sollten Sie bereits Benutzern EBICS-Teilnehmer zugeordnet haben, so sehen sie diese in der Tabelle.

Klicken Sie auf die Schaltfläche **NEU**.

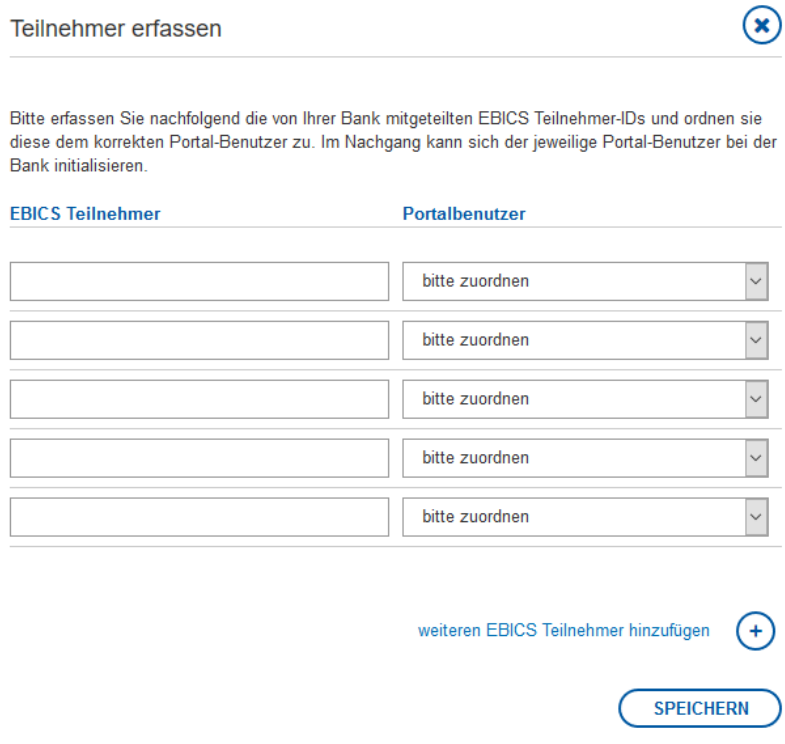

Abbildung 24: Neue EBICS-Teilnehmer zu Benutzern zuordnen

Der sich nun öffnende Dialog **Teilnehmer erfassen** unterscheidet sich je nachdem, ob es sich um den Bankparameter der Aareal Bank oder einer anderen Bank handelt Im ersten Fall werden Ihnen die EBICS-Teilnehmer mit ihren Bezeichnungen angeboten und müssen lediglich den zugehörigen Portalbenutzern aus der Aufklappliste der rechten

Spalte zugeordnet werden. Handelt es sich dagegen um den Bankparameter einer anderen Bank, so sind die EBICS Teilnehmer-IDs einzeln einzutragen, bevor sie den Portalbenutzern zugeordnet werden können. Wiederholen Sie diesen Schritt, bis alle Benutzer zugeordnet sind und **SPEICHERN** Sie Ihre Einstellungen.

Fahren Sie dann mit der Zuordnung von EBICS-Teilnehmern zu Benutzern für Ihre weiteren Bankparameter fort.

Bitte denken Sie abschließend daran, Ihre Benutzer zu informieren, wie Sie Ihre EBICS-Teilnehmer initialisieren können. Kapitel 6.2.3 im Benutzerhandbuch beschreibt die Vorgehensweise durch die Verwendung des Initialisierungsassistenten.

9. Abrufmanager

Mit Hilfe des Abrufmanagers können Sie Kontoauszüge, Mitteilungen Ihrer Bank und andere Informationen abrufen und diese im Postfach hinterlegen.

Der Abrufmanager ist eine Funktion, die allen Portalbenutzern zur Verfügung steht. Abrufe sind grundsätzlich von allen Benutzern konfigurierbar und für alle Benutzer sichtbar. Ebenso stehen die durch die Abrufe im Postfach bzw. im Bereich der Protokolle abgelegten Informationen allen Benutzern zur Verfügung. Die Bedienung des Abrufmanagers ist daher im Benutzerhandbuch in Kapitel 6.3 beschrieben.

Sollten Sie sich dafür entscheiden, die Konfiguration des Abrufmanagers zentral vorzunehmen, so schränken Sie den Zugriff auf den Abrufmanager mit Hilfe von Rollendefinitionen ein. Die genaue Vorgehensweise hierfür ist in Kapitel 6.1 beschrieben.

10. Aktivitätenprotokolle

In den Aktivitätenprotokollen dokumentiert das Aareal Portal alle wichtigen Aktionen, die Sie oder einer der von Ihnen verwalteten Benutzer im Aareal Portal ausgeführt haben. Dies können z. B. sein:

- An- und Abmeldungen von Benutzern am Aareal Portal
- Anlegen oder Löschen von *EBICS*-Teilnehmern
- Erstellung oder Unterschrift von Zahlungsaufträgen
- Anlage von Postfächern
- Anlage, Änderung oder das Löschen von Mandaten
- Anlage, Sperren, Beendigung von Benutzern
- usf.

Die Aktivitätenprotokolle sind im Aareal Portal für maximal 24 Monate zur Einsicht verfügbar und werden anschließend gelöscht. Es kann ggf. eine kürzere Löschfrist geben. Die Aktivitätenprotokolle erreichen Sie über das Modul **ADMINISTRATION** ▶ **PROTOKOLLE** ▶ **AKTIVITÄTENPROTOKOLLE**.

Neben **Datum** und Zeitpunkt der durchgeführten Aktivität sehen Sie in der Übersicht auch Details wie die Referenznummer des Mandats oder den angelegten EBICS-Teilnehmer.

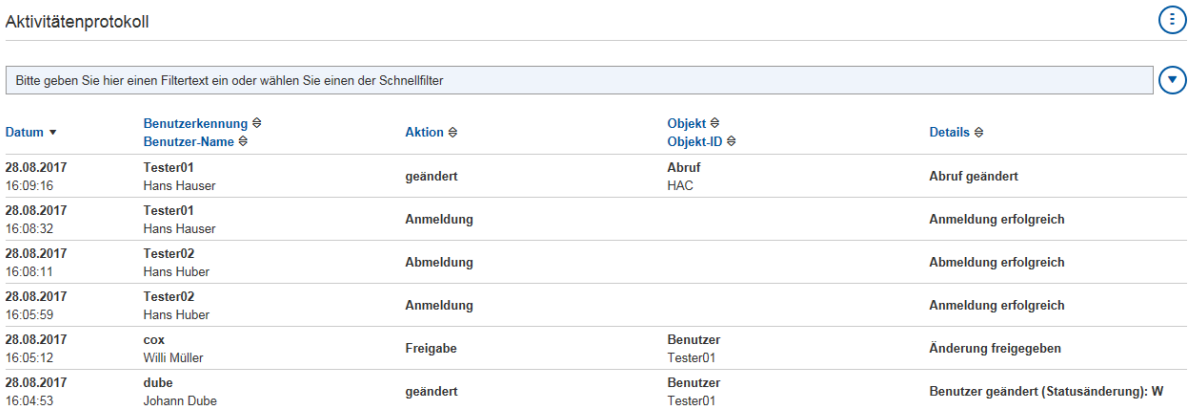

Abbildung 25: Die Ansicht der Aktivitätenprotokolle

Falls Sie mehr Informationen zur jeweiligen Aktion erfahren möchten, klicken Sie auf den entsprechenden Zeileneintrag. Die folgende Abbildung zeigt die Detailinformationen zu einem neu angelegten Mandat.

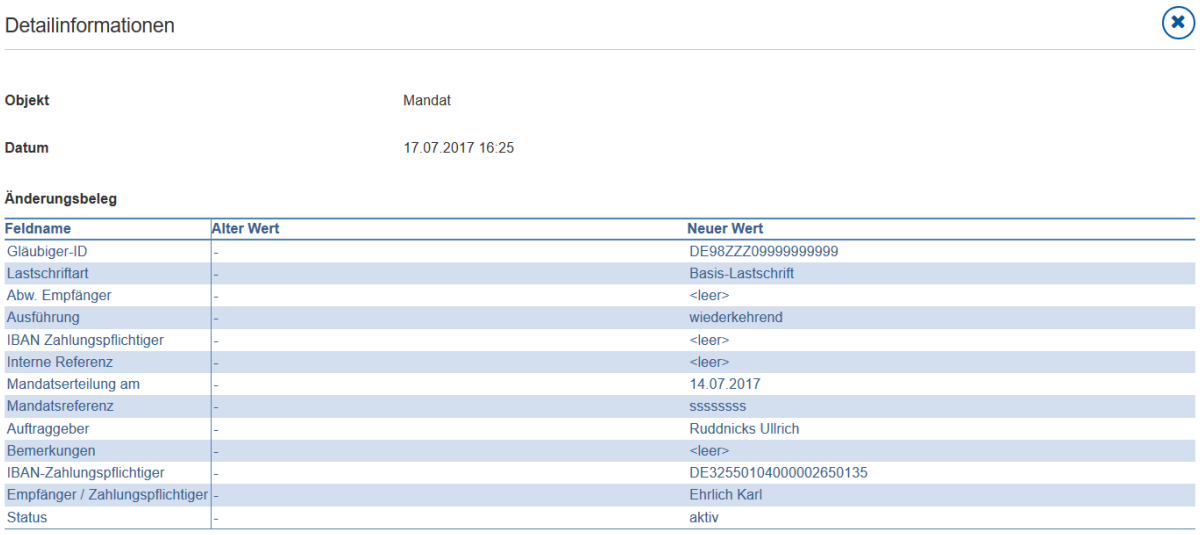

Abbildung 26: Weitere Detailinformationen im Aktivitätenprotokoll am Beispiel eines neu angelegten Mandats

! ***Hinweis:*** *Für einen gelöschten Partner aus dem Adressbuch werden in den Protokolleinträgen des Aktivitätenprotokolls keine Detailinformationen (Partnerdaten) und somit keine DSGVO-relevanten Daten angezeigt.*

11. Abbildungsverzeichnis

Abbildung 1: Darstellung der Stammdaten in der Benutzerverwaltung 14
Abbildung 2: Benutzer eines Kundenzugangs 16
Abbildung 3: Aktionen zum Sperren, Löschen, Ändern und Anfordern neuer Zugangsdaten 18
Abbildung 4: Einen neuen Benutzer anlegen – Eingabe der Stammdaten 19
Abbildung 5: Einen neuen Benutzer anlegen – Schlüsselmedium hinterlegen 20
Abbildung 6: Ein aktiviertes Schlüsselmedium mit Möglichkeit zum Widerruf 21
Abbildung 7: Einen neuen Benutzer anlegen – Module auswählen und Rollen festlegen 22
Abbildung 8: Einen neuen Benutzer anlegen – Kontoeinschränkungen festlegen.....23
Abbildung 9: Hinweistext eines gesperrten Benutzers 24
Abbildung 10: Freigabe eines Schlüsselmediums mit Hilfe des Freigabecodes 26
Abbildung 11: Änderung des eigenen Benutzerpassworts 27
Abbildung 12: Übersicht über vorhandene Rollen 29
Abbildung 13: Ein Ausschnitt des Dialogs zum Anlegen einer neuen Rolle 30
Abbildung 14: Übersicht Ihrer Vorlagen für Kontoeinschränkungen 32
Abbildung 15: Dialog zur Anlage einer neuen Kontoeinschränkung.....32
Abbildung 16: Übersicht über alle aktivierten imageTAN-Reader 35
Abbildung 17: Einstellungen am imageTAN-Reader 36
Abbildung 18: Die Seite für den Login 38
Abbildung 19: Entsperrung des imageTAN-Readers mit Hilfe des Entsperrcodes 38
Abbildung 20: Der Freigabecode zur Vergabe einer neuen PIN 39
Abbildung 21: Sicherheitsabfrage vor dem Sperren des imageTAN-Readers.....40
Abbildung 22: Invalidierung eines imageTAN-Readers im Reiter Schlüsselmedium 40
Abbildung 23: Zuordnung von EBICS-Teilnehmern zu Benutzern 43
Abbildung 24: Neue EBICS-Teilnehmer zu Benutzern zuordnen 43
Abbildung 25: Die Ansicht der Aktivitätenprotokolle 46
Abbildung 26: Weitere Detailinformationen im Aktivitätenprotokoll am Beispiel eines neu angelegten Mandats 47

12. Tabellenverzeichnis

Tabelle 1: Stammdaten des Kundenzugangs 15
Tabelle 2: Mögliche Status eines Benutzerzugangs 17
Tabelle 3: Mögliche Status des Schlüsselmediums 17